Von dem Fachbereich
für Mathematik und Informatik
der Technischen Universität Braunschweig

genehmigte Dissertation

zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)

Jörn Sommer

Diophantische Methoden bei der expliziten Lösung von Einbettungsproblemen in der Galoistheorie

Braunschweig, 16. Oktober 1998

Von dem Fachbereich
für Mathematik und Informatik
der Technischen Universität Braunschweig

genehmigte Dissertation

zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)

Jörn Sommer

Diophantische Methoden bei der expliziten Lösung von Einbettungsproblemen in der Galoistheorie

Braunschweig, 16. Oktober 1998

1. Referent: Prof. Dr. rer. nat. H. Opolka
2. Referent: PD Dr. rer. nat. P. Schroth
Eingereicht am: 14. Juli 1998

Meiner Mutter, meinem Vater

Inhaltsverzeichnis

Kapitel 1

Einleitung

Unter dem bis heute ungelösten *Umkehrproblem der Galoistheorie* versteht man die Frage, ob es zu jeder endlichen Gruppe G einen Erweiterungskörper K des Körpers $\mathbb{Q}$ der rationalen Zahlen gibt, so daß $K/\mathbb{Q}$ galoissch mit zu G isomorpher Galoisgruppe ist.

Die Frage, die den Ausgangspunkt sowohl für diese Dissertation als auch schon für die Diplomarbeit darstellte, ist eine leicht abgewandelte: Dazu gebe man sich eine endliche Galoiserweiterung K/k mit Galoisgruppe G und eine endliche Gruppenerweiterung E von G vor.

> Gibt es eine galoissche Erweiterung $L/K/k$ derart, daß die Galoisgruppe von L/k isomorph zu E ist und die galoistheoretische Restriktionsabbildung $\mathrm{G}(L/k) \to \mathrm{G}(K/k)$ mit dem gegebenen Epimorphismus $E \to G$ übereinstimmt?

Dies ist – zusammen mit einigen zusätzlichen Forderungen – die galoistheoretische Interpretation eines *Einbettungsproblems*.

Konkret wurde in der Diplomarbeit untersucht, ob es ein Lösbarkeitskriterium in Form einer Normgleichung gibt. Man entscheidet also die Lösbarkeit eines Einbettungsproblems, indem man feststellt, ob ein gewisses Element sich als Norm in der Erweiterung K/k schreiben läßt, d.h. ob das Element im Bild der körpertheoretischen Normabbildung $\mathrm{N}_{K/k}$ liegt. Für zyklische Gruppen G war das bekannt. In der Diplomarbeit ging es darum, für abelsche (nicht-zyklische) Gruppen ein solches

Kriterium zu finden; dies wurde im Fall einer Gruppe G vom Typ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dort angegeben.

Die Aufgabenstellung für diese Arbeit wurde dahingehend erweitert, daß man nicht nur ein Lösbarkeitskriterium, sondern zusätzlich auch ein Konstruktionsverfahren für explizite Lösungskörper erhalten möchte.

Ein Beispiel von SERRE aus [Ser 92] soll diese Zielsetzung verdeutlichen. Sei k ein Körper der Charakteristik $\operatorname{char} k \neq 2$. Sei L/k eine zyklische Galoiserweiterung vom Grad 4, d.h.

$$\mathrm{G}(L/k) \cong \mathbb{Z}/4\mathbb{Z}.$$

Die Erweiterung L erhält man durch einen eindeutig bestimmten Turm quadratischer Erweiterungen $k \subset K \subset L$, wobei

$$K = k(\sqrt{\varepsilon}) \qquad \text{und} \qquad L = K(\sqrt{a + b\sqrt{\varepsilon}})$$

mit $\varepsilon \in k^\times - {k^\times}^2$ und $a, b \in k^\times$ ist. Im allgemeinen ist L/k allerdings nicht galoissch: Zum Beispiel sind für $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$ die Teil-Erweiterungen L/K und K/k zwar galoissch, aber L/k ist nicht normal.

Satz 1.1 (Serre)

L/k ist genau dann eine zyklische Galoiserweiterung vom Grad 4, wenn ein $c \in k^\times$ mit $a^2 - \varepsilon b^2 = \varepsilon c^2$ existiert.

Beweis:

[Ser 92], Chapter 1.2, Thm. 1.2.1 □

Die zyklischen Körpererweiterungen vom Grad 4 eines Körpers der Charakteristik $\neq 2$ werden also parametrisiert durch die Lösungen (ε, a, b, t) der Gleichung

$$a^2 - \varepsilon b^2 = \varepsilon t^2 \tag{1.1}$$

mit $t \neq 0$ und ε kein Quadrat. Diese Gleichung repräsentiert eine rationale Varietät: man kann sie für ε in Abhängigkeit von a, b und t lösen. Man beachte, daß die linke Seite gerade die Norm

$$\mathrm{N}_{L/K}(a + b\sqrt{\varepsilon}) = a^2 - \varepsilon b^2$$

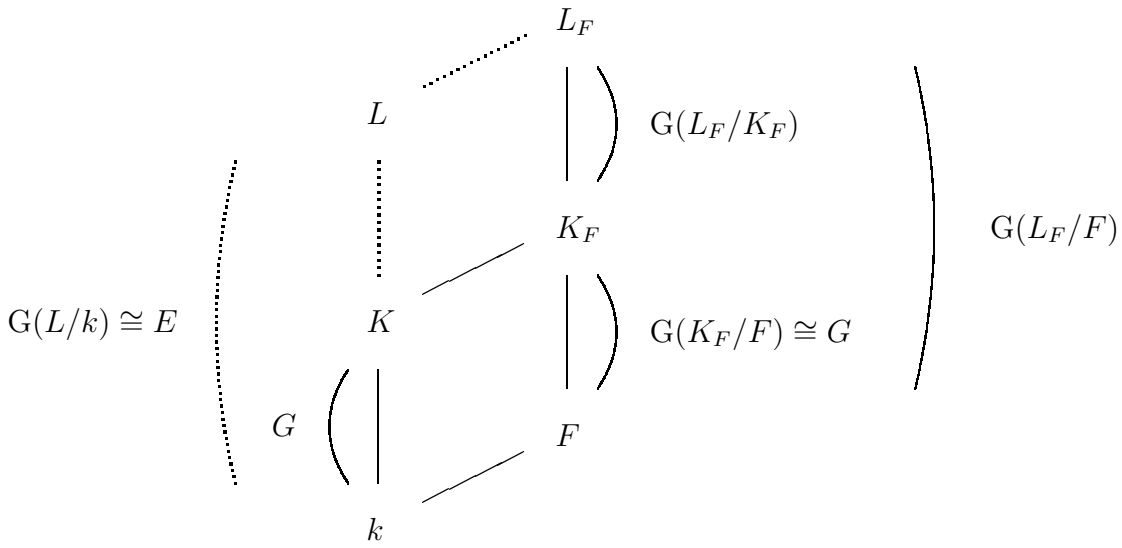
ist. Wie oben bereits erwähnt wurde, existiert bei zyklischen Galoisgruppen stets ein Normkriterium.

In dem eben beschriebenen Fall wird also das Hindernis für die Lösbarkeit eines vorgegebenen Einbettungsproblems durch eine Varietät beschrieben. Kann man auf ihr einen rationalen Punkt finden, so ist das Einbettungsproblem lösbar. Zudem – und das ist der entscheidende Punkt – kann man die gesuchte Körpererweiterung mittels dieser Lösung sogar explizit angeben.

Der Ansatz dieser Arbeit bestand darin, dieses Beispiel mit Hilfe der Ergebnisse der Diplomarbeit auch auf nicht-zyklische Galoiserweiterungen zu verallgemeinern. Dabei ist die Grundidee, daß man Unbestimmte, also transzendente Elemente, einführt, mit deren Hilfe man das gegebene Einbettungsproblem erst einmal 'virtuell' löst. Man verschiebt das Problem quasi und geht zunächst zu gewissen Funktionenkörpern über, die die vorteilhafte Eigenschaft besitzen, daß über ihnen als Grundkörper das Einbettungsproblem lösbar ist. Dafür kommen die sogenannten *Brauerkörper* in Betracht. Anschließend konstruiert man einen virtuellen Lösungskörper.

Für den nächsten Schritt setze man voraus, daß das Einbettungsproblem als Lösbarkeitskriterium eine Normgleichung (etwa von der Form (1.1)) habe, die man als Varietät deutet. Man schiebt das Problem wieder zurück, indem man die Unbestimmten in dem virtuellen Lösungskörper durch *Spezialisierung* ersetzt: Man versucht, Werte für die Unbestimmten derart zu finden, daß die berechnete Varietät einen rationalen Punkt hat. Denn das ist gleichbedeutend mit der Lösbarkeit des Einbettungsproblems. Diese Spezialisierung überträgt man auf den virtuellen Lösungskörper und gewinnt auf diese Weise einen expliziten Lösungskörper ohne Unbestimmte.

Anhand des folgenden Diagramms läßt sich die Problemstellung verdeutlichen:



In der linken Hälfte stehen die expliziten Erweiterungen, rechts die virtuellen. Man startet also links mit der Erweiterung K/k mit Galoisgruppe G und sucht nach einer Erweiterung $L/K/k$, so daß $\mathrm{G}(L/k)$ isomorph zu der durch das Einbettungsproblem vorgegebenen Gruppe E ist. Man konstruiert zunächst den Brauerkörper F und beweist, daß die Galoisgruppe von $K_F = FK$ über F isomorph zu G ist und daß das Einbettungsproblem über dem Grundkörper F – sozusagen virtuell – lösbar ist. Durch die Spezialisierung der Unbestimmten in dem virtuellen Lösungskörper L_F, der über F eine zu E isomorphe Galoisgruppe hat, gewinnt man den expliziten Lösungskörper L und gelangt somit wieder zurück in die linke Hälfte des Diagramms.

Der Verlauf der Arbeit soll kurz skizziert werden. Im nächsten Kapitel werden die wichtigsten Grundlagen erklärt, wobei der Schwerpunkt auf kohomologische Aspekte gesetzt wird, ergänzt durch einen Abriß über die Diplomarbeit. Danach werden Brauerkörper definiert und ihr Zusammenhang zu Einbettungsproblemen dargestellt. Im vierten Kapitel wird das Verfahren theoretisch beschrieben. Im fünften und letzten Kapitel wird anhand eines Gegenbeispiels zum Hasseschen Normensatz auf die praktische Umsetzung der Theorie eingegangen und obiges Beispiel von Serre noch einmal aufgegriffen, womit sich der Kreis dieser Arbeit schließt.

Mein herzlicher Dank gebührt Herrn Prof. Dr. H. Opolka für die Betreuung und den Einsatz an Zeit und Mühe. Seine nachhaltige Unterstützung, seine wissenschaftlichen Anregungen und seine fortwährende Aufgeschlossenheit auftretenden Fragen gegenüber waren mir eine unschätzbare Hilfe.

Kapitel 2

Grundlagen

In diesem Kapitel sollen die grundlegenden Begriffe für diese Arbeit beschrieben werden. Zunächst werden die Kohomologiegruppen eingeführt. Es folgen die Definitionen eines (zentralen) Einbettungsproblems und der Brauergruppe eines Körpers, deren Zusammenhang anschließend dargestellt wird. Abgeschlossen wird das Kapitel mit den Ergebnissen aus der Diplomarbeit.

2.1 Kohomologie

Ein *Komplex* $\mathcal{K} = (E, d)$ ist eine Familie $\{E^n \mid n \in \mathbb{Z}\}$ von abelschen Gruppen zusammen mit Homomorphismen $d^n : E^n \to E^{n+1}$, für die $d^{n+1} \circ d^n = 0$ gilt, d.h. $\operatorname{Bild} d^n \subseteq \operatorname{Kern} d^{n+1} \subseteq E^{n+1}$ für alle $n \in \mathbb{Z}$. Die *n-te Kohomologiegruppe* eines Komplexes $\mathcal{K}$ ist definiert als

$$\mathrm{H}^n(\mathcal{K}) := \operatorname{Kern} d^n \,/\, \operatorname{Bild} d^{n-1} \qquad (n \in \mathbb{Z}).$$

Ein *Morphimus* $\phi : \mathcal{K} \to \mathcal{K}' = (E', d')$ von Komplexen ist ein Funktor von Homomorphismen $\phi^n : E^n \to E'^n$, so daß $d'^n \circ \phi^n = \phi^{n+1} \circ d^n$ gilt. Begriffe wie Kern, Bild oder exakte Sequenz übertragen sich in natürlicher Weise von der Kategorie der abelschen Gruppen auf die Kategorie der Komplexe. Es gilt (siehe [P-S 92], Appendix 1, Ch. 1.4):

(a) Ein Morphismus $\phi : \mathcal{K} \to \mathcal{K}'$ induziert einen Homomorphismus $\phi^* : \mathrm{H}^n(\mathcal{K}) \to \mathrm{H}^n(\mathcal{K}')$ (für alle $n \in \mathbb{Z}$).

(b) Eine kurze exakte Sequenz von Komplexen

$$0 \longrightarrow \mathcal{K}_1 \xrightarrow{\phi_1} \mathcal{K}_2 \xrightarrow{\phi_2} \mathcal{K}_3 \longrightarrow 0$$

induziert eine unendlich lange exakte Kohomologiesequenz

$$\begin{array}{lllll} \ldots & \xrightarrow{\Delta^{n-1}} & \mathrm{H}^n(\mathcal{K}_1) & \xrightarrow{\phi_1^*} & \mathrm{H}^n(\mathcal{K}_2) \xrightarrow{\phi_2^*} \mathrm{H}^n(\mathcal{K}_3) \\ & \xrightarrow{\Delta^n} & \mathrm{H}^{n+1}(\mathcal{K}_1) & \xrightarrow{\phi_1^*} & \ldots \quad . \end{array}$$

Konstruktion des Verbindungshomomorphismus Δ^n

Sei $(z) \in \mathrm{H}^n(\mathcal{K}_3)$, also $z \in E_3^n$ mit $d_3^n(z) = 0$. Die kurze exakte Sequenz liefert ein $y \in E_2^n$ mit $\phi_2^n(y) = z$ ist. Es folgt

$$(\phi_2^{n+1} \circ d_2^n)(y) = (d_3^n \circ \phi_2^n)(y) = d_3^n(z) = 0.$$

Wegen der Exaktheit bei $\mathcal{K}_2$ existiert ein $x \in E_1^{n+1}$ mit $\phi_1^{n+1}(x) = d_2^n(y)$ und

$$(\phi_1^{n+2} \circ d_1^{n+1})(x) = (d_2^{n+1} \circ \phi_1^{n+1})(x) = (d_2^{n+1} \circ d_2^n)(y) = 0.$$

Die Injektivität von ϕ_1^{n+2} erzwingt $d_1^{n+1}(x) = 0$. Die Klasse $(x) \in \mathrm{H}^{n+1}(\mathcal{K}_1)$ ist unabhängig von der Wahl der x, y und des Repräsentanten aus (z). Somit erhält man einen wohldefinierten Homomorphismus

$$\Delta^n \ : \ \mathrm{H}^n(\mathcal{K}_3) \longrightarrow \mathrm{H}^{n+1}(\mathcal{K}_1) \ : \ (z) \longmapsto (x).$$

(c) Δ^n ist funktoriell in dem folgenden Sinn:
Ist das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{K}_1 & \longrightarrow & \mathcal{K}_2 & \longrightarrow & \mathcal{K}_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{K}_1' & \longrightarrow & \mathcal{K}_2' & \longrightarrow & \mathcal{K}_3' & \longrightarrow & 0 \end{array}$$

mit exakten Zeilen kommutativ, so ist auch

$$\begin{array}{ccc} \mathrm{H}^n(\mathcal{K}_3) & \xrightarrow{\Delta^n} & \mathrm{H}^{n+1}(\mathcal{K}_1) \\ \downarrow & & \downarrow \\ \mathrm{H}^n(\mathcal{K}_3') & \xrightarrow{\Delta'^n} & \mathrm{H}^{n+1}(\mathcal{K}_1') \end{array}$$

kommutativ.

Sei $\mathcal{G}$ eine *proendliche Gruppe*, d.h. $\mathcal{G}$ läßt sich als projektiver Limes endlicher Gruppen darstellen. Unter einem *(diskreten) $\mathcal{G}$-Modul* A versteht man eine abelsche Gruppe A, die zugleich als topologischer Raum die diskrete Topologie trägt, zusammen mit einer stetigen Abbildung

$$\mathcal{G} \times A \longrightarrow A : \ (\sigma, a) \longmapsto \sigma a,$$

der *Operation* von $\mathcal{G}$ auf A, die die Bedingungen

$$1_{\mathcal{G}}\, a = a, \quad (\sigma\tau)\, a = \sigma\,(\tau\, a) \quad \text{und} \quad \sigma\,(a+b) = \sigma\, a + \sigma\, b$$

für alle $\sigma, \tau \in \mathcal{G},\ a, b \in A$ erfüllt. Ein *Morphismus* $\phi : A \to B$ von zwei $\mathcal{G}$-Moduln A, B ist ein (stetiger) $\mathcal{G}$-Homomorphismus, d.h. es gilt

$$\phi(\sigma a) = \sigma\phi(a) \qquad (\sigma \in \mathcal{G},\ a \in A),$$

so daß die Menge der $\mathcal{G}$-Moduln eine Kategorie bildet. Der *Fixmodul* von A unter der Operation von $\mathcal{G}$ ist die Menge $A^{\mathcal{G}} := \{a \in A \mid \sigma a = a \ \ \forall\ \sigma \in \mathcal{G}\}$. Aus formalen Gründen wird in diesem Teil die additive Schreibweise von A vorgezogen, doch in den meisten Anwendungen wird A multiplikativ aufgefaßt, so daß obige Bedingungen die Gestalt

$$a^{1_{\mathcal{G}}} = a, \qquad a^{\sigma\tau} = (a^{\tau})^{\sigma} \qquad \text{und} \qquad (ab)^{\sigma} = a^{\sigma} b^{\sigma}$$

annehmen. Als Standard-Beispiel sei der Fall erwähnt, daß $\mathcal{G}$ die Galoisgruppe $\mathrm{G}(K/k)$ einer Körpererweiterung K/k und A die multiplikative Gruppe $K^{\times}$ ist. Dann ist die Operation durch

$$a^{\sigma} := \sigma(a) \qquad (\sigma \in \mathrm{G}(K/k), a \in K^{\times})$$

erklärt. Hier ist der Fixmodul $A^{\mathcal{G}} = k^{\times}$.

Für eine proendliche Gruppe $\mathcal{G}$ und einen $\mathcal{G}$-Modul A heißen die Elemente aus

$$\begin{aligned} \mathrm{C}^n(\mathcal{G}, A) &:= \{f : \mathcal{G}^n \longrightarrow A \mid f \text{ stetig}\} \qquad (n \in \mathbb{N}), \\ \mathrm{C}^0(\mathcal{G}, A) &:= A \end{aligned}$$

n-Koketten. Bei multiplikativ aufgefaßtem A schreibt man häufig $f_{\sigma_1,\ldots,\sigma_n}$ statt $f(\sigma_1, \ldots, \sigma_n)$. Durch punktweise Übertragung der Addition von A auf $\mathrm{C}^n(\mathcal{G}, A)$ werden diese zu abelschen Gruppen. Für $n \in \mathbb{N}_0$ ist die *n-te Korandabbildung*

$$d_n \;:\; \mathrm{C}^n(\mathcal{G}, A) \longrightarrow \mathrm{C}^{n+1}(\mathcal{G}, A) \;:\; f \longmapsto d_n f$$

durch

$$\begin{aligned}(d_n f)(\sigma_1, \ldots, \sigma_{n+1}) \quad &:= \quad \sigma_1 \, f(\sigma_2, \ldots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i \, f(\sigma_1, \ldots, \sigma_i \sigma_{i+1}, \ldots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} \, f(\sigma_1, \ldots, \sigma_n)\end{aligned} \tag{2.1}$$

definiert. Es gilt $d_{n+1} \circ d_n = 0$ für $n \in \mathbb{N}$ (siehe [A-I 95], Thm. 5.5.1).

Die Familie $\mathrm{C}^*(\mathcal{G}, A) := \{\mathrm{C}^n(\mathcal{G}, A), d_n\}$ ist ein Komplex, wenn man $\mathrm{C}^n(\mathcal{G}, A) := 0$ und $d_n := 0$ für $n = -1, -2, \ldots$ setzt.

Definition 2.1

Sei $n \in \mathbb{N}_0$. Die n-te Kohomologiegruppe von $\mathcal{G}$ mit Koeffizienten in A wird mit

$$\begin{aligned}\mathrm{H}^n(\mathcal{G}, A) \;&:=\; \mathrm{H}^n(\mathrm{C}^*(\mathcal{G}, A)) \\ &=\; \operatorname{Kern} d_n \,/\, \operatorname{Bild} d_{n-1}\end{aligned}$$

bezeichnet.
Die Elemente aus $\mathrm{Z}^n(\mathcal{G}, A) := \operatorname{Kern} d_n$ heißen n-Kozykeln, jene aus $\mathrm{B}^n(\mathcal{G}, A) := \operatorname{Bild} d_{n-1}$ n-Koränder.
Zwei n-Kozykeln f, f' heißen kohomolog, wenn ihre Äquivalenzklassen $(f), (f')$ in $\mathrm{H}^n(\mathcal{G}, A)$ übereinstimmen. (f) heißt die Kozykelklasse von f.

Verwendet man (2.1), so erhält man in den Dimensionen $0, 1$ und 2 die folgenden Kohomologiegruppen – dabei seien $\sigma, \tau, \rho \in \mathcal{G}$ stets beliebig:

(a) $\mathrm{Z}^0(\mathcal{G}, A) = \{a \in \mathrm{C}^0(\mathcal{G}, A) = A \mid \sigma a - a = 0\} = A^{\mathcal{G}}$
$\mathrm{B}^0(\mathcal{G}, A) = 0$
$\Longrightarrow \quad \mathrm{H}^0(\mathcal{G}, A) = A^{\mathcal{G}}$

(b) $\mathrm{Z}^1(\mathcal{G}, A) = \{\lambda \in \mathrm{C}^1(\mathcal{G}, A) \mid \lambda(\sigma\tau) = \sigma\lambda(\tau) + \lambda(\sigma)\}$
$\mathrm{B}^1(\mathcal{G}, A) = \{\kappa \in \mathrm{C}^1(\mathcal{G}, A) \mid \exists\, a \in A : \quad \kappa(\sigma) = \sigma a - a\}$
Operiert $\mathcal{G}$ trivial auf A, so ist $\mathrm{H}^1(\mathcal{G}, A) = \mathrm{Hom}_{\mathrm{cts}}(\mathcal{G}, A)$ die Menge der stetigen Gruppenhomomorphismen von $\mathcal{G}$ nach A.

(c) $\mathrm{Z}^2(\mathcal{G},A) = \{f \in \mathrm{C}^2(\mathcal{G},A) \mid f(\sigma\tau,\rho) + f(\sigma,\tau) = \sigma\, f(\tau,\rho) + f(\sigma,\tau\rho)\}$
$\mathrm{B}^2(\mathcal{G},A) = \{g \in \mathrm{C}^2(\mathcal{G},A) \mid \exists\ \lambda \in \mathrm{C}^1(\mathcal{G},A) :\ g(\sigma,\tau) = \sigma\,\lambda(\tau) - \lambda(\sigma\tau) + \lambda(\sigma)\}$

Ist $\mathcal{U} \leq \mathcal{G}$ eine Untergruppe von $\mathcal{G}$ und $n \in \mathbb{N}_0$, so heißt die Abbildung

$$\mathrm{res}^{\mathcal{G}}_{\mathcal{U}}\ :\ \mathrm{H}^n(\mathcal{G},A) \longrightarrow \mathrm{H}^n(\mathcal{U},A)\ :\ (f) \longmapsto \mathrm{res}^{\mathcal{G}}_{\mathcal{U}}((f)) := (\tilde{f}) \tag{2.2}$$

mit $\tilde{f}(\sigma_1,\ldots,\sigma_n) := f|_{\mathcal{U}}(\sigma_1,\ldots,\sigma_n)$ die *(kohomologische) Restriktion*. Ist $\mathcal{N} \leq \mathcal{G}$ ein abgeschlossener Normalteiler von $\mathcal{G}$ und bezeichne $\bar{\sigma}$ das Bild von σ unter dem natürlichen Epimorphismus $\mathcal{G} \to \mathcal{G}/\mathcal{N}$, so ist

$$\mathrm{inf}^{\mathcal{G}/\mathcal{N}}_{\mathcal{G}}\ :\ \mathrm{H}^n(\mathcal{G}/\mathcal{N},A^{\mathcal{N}}) \longrightarrow \mathrm{H}^n(\mathcal{G},A)\ :\ (f) \longmapsto \mathrm{inf}^{\mathcal{G}/\mathcal{N}}_{\mathcal{G}}((f)) := (\bar{f}) \tag{2.3}$$

mit $\bar{f}(\sigma_1,\ldots,\sigma_n) := f(\bar{\sigma}_1,\ldots,\bar{\sigma}_n)$ die *Inflation*.

In dem Fall, daß $\mathcal{G}$ eine endliche Gruppe G ist, lassen sich auch für negatives n Kohomologiegruppen

$$\hat{\mathrm{H}}^n(G,A)$$

definieren. Diese *Tate'schen Kohomologiegruppen* sind in den Dimensionen $n > 0$ identisch mit den oben eingeführten $\mathrm{H}^n(G,A)$. Für $n = 0$ ist $\mathrm{B}^0(G,A) = \mathrm{N}_G(A)$, wobei d_{-1} der *Normabbildung* $\mathrm{N}_G :\ A \to A :\ a \mapsto \sum_{\sigma\in G} \sigma a$ entspricht, so daß

$$\hat{\mathrm{H}}^0(G,A) = A^G/\mathrm{N}_G(A)$$

ist (siehe auch [P-S 92], Chap. 2.3.8). Ist K/k eine endliche Körpererweiterung mit Galoisgruppe G, so wird N_G zur körpertheoretischen Normabbildung

$$\mathrm{N}_{K/k} :\ K \longrightarrow k\ :\ x \longmapsto \prod_{\sigma\in G} \sigma(x).$$

Von Bedeutung ist der folgende

Satz 2.2 (Hilbert 90)

Sei k ein Körper und K/k eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{G}(K/k)$. Dann ist

$$\mathrm{H}^1(G,K^\times) = 1.$$

Beweis:

Sei $\lambda \in \mathrm{Z}^1(G, K^\times)$ beliebig. Nach einem Satz von E. ARTIN (siehe [Lor 92], §12, Satz 2′) sind die k-Automorphismen $\tau \in G$ linear unabhängig über K. Daher existiert ein $\theta \in K^\times$, so daß

$$\beta := \sum_{\tau \in G} \lambda_\tau \, \theta^\tau$$

ungleich Null ist. Für alle $\sigma \in G$ gilt

$$\beta^\sigma = \sum_{\tau \in G} \lambda_\tau^\sigma \, (\theta^\tau)^\sigma = \sum_{\tau \in G} \lambda_{\sigma\tau} \lambda_\sigma^{-1} \, \theta^{\sigma\tau} = \lambda_\sigma^{-1} \sum_{\rho \in G} \lambda_\rho \, \theta^\rho = \lambda_\sigma^{-1} \beta,$$

so daß mit $c := \beta^{-1}$

$$\lambda_\sigma = \frac{c^\sigma}{c} \qquad (\sigma \in G)$$

folgt. Also liegt λ bereits in $\mathrm{B}^1(G, K^\times)$. □

Durch Übergang zum induktiven Limes stellt man fest, daß Hilbert 90 auch für beliebige (unendliche) Galoiserweiterungen K/k gilt (siehe [Lor 93], Satz 8.1.6). Insbesondere ist für die *absolute Galoisgruppe* $\mathcal{G}_k = \mathrm{G}(\overline{k}/k)$ eines separabel-algebraischen Abschlusses $\overline{k}$ über k

$$\mathrm{H}^1(\mathcal{G}_k, \overline{k}^\times) = 1. \tag{2.4}$$

Die Kohomologie-Theorie proendlicher Gruppen $\mathcal{G}$ läßt sich in den Dimensionen 0 und 1 auf nicht-abelsche Koeffizientengruppen ausdehnen. Eine $\mathcal{G}$-*Menge* A ist ein diskreter topologischer Raum, auf dem $\mathcal{G}$ stetig operiert, und man definiert

$$\mathrm{H}^0(\mathcal{G}, A) := A^{\mathcal{G}}.$$

Ist A eine (multiplikativ geschriebene, nicht-abelsche) $\mathcal{G}$-*Gruppe*, d.h. eine Gruppe mit einer $\mathcal{G}$-Operation, so ist ein 1-Kozykel auf $\mathcal{G}$ mit Werten in A eine stetige Abbildung $\lambda : \mathcal{G} \to A : \sigma \mapsto \lambda_\sigma$ mit

$$\lambda_{\sigma\tau} = \lambda_\sigma \, \lambda_\tau^\sigma \qquad (\sigma, \tau \in \mathcal{G}). \tag{2.5}$$

Zwei 1-Kozykeln λ, λ' sind *kohomolog*, wenn ein $a \in A$ mit

$$\lambda'_\sigma = a^{-1}\,\lambda_\sigma\,a^\sigma \qquad (\sigma \in \mathcal{G}) \tag{2.6}$$

existiert. Die *erste Kohomologiemenge* $\mathrm{H}^1(\mathcal{G}, A)$ von $\mathcal{G}$ mit Werten in A ist die Menge der Äquivalenzklassen. Im allgemeinen ist also $\mathrm{H}^1(\mathcal{G}, A)$ für eine nicht-abelsche $\mathcal{G}$-Gruppe A keine Gruppe, sondern lediglich eine *Menge mit einem ausgezeichneten Element*, nämlich der Äquivalenzklasse von $\lambda^\circ :\ \mathcal{G} \to A :\ \sigma \mapsto \lambda^\circ_\sigma := 1$.

Unter einer *exakten Sequenz von Mengen mit ausgezeichnetem Element* versteht man eine Folge von Mengenabbildungen, bei denen jeweils das ausgezeichnete Element auf das ausgezeichnete Element abgebildet wird und das Bild einer Abbildung mit dem Urbild des ausgezeichneten Elementes der nachfolgenden Abbildung übereinstimmt. Die Definition der Korandabbildungen d_n und der Verbindungshomomorphismen Δ^n verlaufen für $n = 0, 1$ analog der abelschen Kohomologie. Explizit ist

$$(d_0 a)(\sigma) = a^{-1}a^\sigma \qquad (a \in A, \sigma \in \mathcal{G})$$

und

$$(d_1\lambda)(\sigma,\tau) = \lambda_\sigma \lambda_\tau^\sigma \lambda_{\sigma\tau}^{-1} \qquad ((\lambda) \in \mathrm{H}^1(\mathcal{G}, A),\ \sigma, \tau \in \mathcal{G}).$$

Eine weitere Verallgemeinerung des vorstehenden Satzes 2.2 erhält man nun (siehe [Ser 95], Chap. X, §1, Prop. 3), indem man $K^\times$ durch die Gruppe $\mathrm{GL}_m(K)$ der invertierbaren $m\times m$-Matrizen mit Einträgen aus K ersetzt, wobei G koeffizientenweise auf den Elementen aus $\mathrm{GL}_m(K)$ operiert, d.h. $a^\sigma = (a_{ij})^\sigma_{i,j=1,\ldots,m} := (a^\sigma_{ij})_{i,j=1,\ldots,m}$ für $a \in \mathrm{GL}_m(K), \sigma \in G$:

$$\mathrm{H}^1(G, \mathrm{GL}_m(K)) = 1. \tag{2.7}$$

2.2 Einbettungsprobleme

Es sei

$$1 \longrightarrow A \xrightarrow{\ i\ } E \xrightarrow{\ \pi\ } G \xrightarrow{\ 1\ } \qquad (*)$$

eine kurze exakte Sequenz von endlichen Gruppen, wobei A als abelsch vorausgesetzt sei. Mit anderen Worten ist $(*)$ eine *Gruppenerweiterung* von G mit abelschem Kern A. Durch $(*)$ wird eine wohldefinierte Operation von G auf A

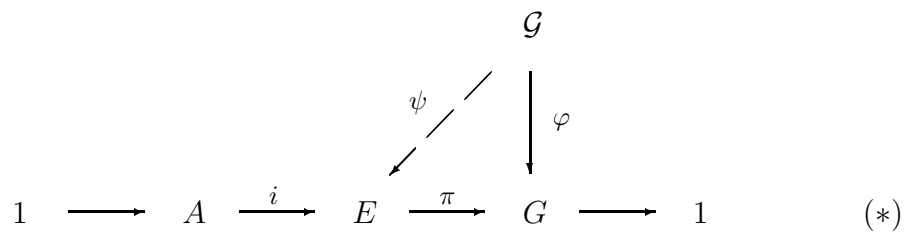
$$a^\sigma := \sigma\, a\, \sigma^{-1} := i^{-1}(\tilde{\sigma}\, i(a)\, \tilde{\sigma}^{-1})$$

für $\sigma \in G, a \in A$ induziert, wobei $\{\tilde{\sigma} \mid \sigma \in G\}$ ein festes Repräsentantensystem von G in E ist.

Definition 2.3

Sei $\mathcal{G}$ eine proendliche Gruppe und $\varphi : \mathcal{G} \to G$ ein surjektiver Homomorphismus. Ein Einbettungsproblem $\mathcal{E}(\mathcal{G}, \varphi, (*))$ für $\mathcal{G}$ wird durch das folgende Diagramm beschrieben:

(2.8)



Gesucht ist dann ein (surjektiver) Homomorphismus $\psi : \mathcal{G} \to E$, der das Diagramm kommutativ ergänzt, für den also gilt: $\pi \circ \psi = \varphi$. Eine Lösung ψ von $\mathcal{E}(\mathcal{G}, \varphi, (*))$ heißt eigentlich, wenn ψ surjektiv ist.
Ist A abelsch und operiert G trivial auf A, so heißt $\mathcal{E}(\mathcal{G}, \varphi, (*))$ ein zentrales Einbettungsproblem.

In der Körper- und Galoistheorie läßt sich das Problem folgendermaßen konkretisieren: Sei k ein Körper mit separabel-algebraischem Abschluß $\overline{k}$. Für $\mathcal{G}$ nehme man die absolute Galoisgruppe $\mathcal{G} = \mathrm{G}(\overline{k}/k)$ von k, welche eine proendliche Gruppe ist. Weiter sei K/k eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{G}(K/k) \cong \mathcal{G}/\mathrm{Kern}\,\varphi$. Dabei ist $\varphi : \mathcal{G} \to G$ die kanonische Projektion, die durch Einschränkung des k-Automorphismus von $\overline{k}$ auf K entsteht. Dann ist das Einbettungsproblem (2.8), also die Suche nach einem surjektiven Homomorphismus $\psi : \mathcal{G} \to E$, gleichbedeutend mit der Suche nach einem Erweiterungskörper $L/K/k$ mit $\mathrm{G}(L/k) \cong E$ derart, daß die kanonische Projektion

$$\mathrm{G}(L/k) \longrightarrow \mathrm{G}(K/k)$$

nach Identifizierung von $\mathrm{G}(L/k)$ bzw. $\mathrm{G}(K/k)$ mit E bzw. G mit

$$\pi \;:\; E \longrightarrow G$$

zusammenfällt. Nach einem Satz von IKEDA (siehe [Ike 60]) gilt über einem algebraischen Zahlkörper k stets: Ist das Einbettungsproblem lösbar, so ist es bereits eigentlich lösbar.

Sei

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1 \qquad (*)$$

eine Erweiterung proendlicher Gruppen mit endlichem abelschen Kern A. Zwei solche Erweiterungen

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1 \qquad (*)$$

und

$$1 \longrightarrow A \xrightarrow{i'} E' \xrightarrow{\pi'} G \longrightarrow 1 \qquad (*)'$$

heißen *isomorph*, wenn es einen Isomorphismus $\phi : E \to E'$ gibt, so daß das Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow\phi & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

kommutativ ist.

Satz 2.4

Es gibt eine Bijektion zwischen den Isomorphieklassen $[(*)]$ von Gruppenerweiterungen von G mit abelschem Kern A und den 2-Kozykelklassen von $\mathrm{H}^2(G, A)$.

Beweis:

Zu $(*)$ existiert ein *stetiger Schnitt* $u : G \to E : \sigma \mapsto u_\sigma$, d.h. es gilt $\pi \circ u = \mathrm{id}_G$, aber u ist i. a. kein Homomorphismus (siehe auch [Shz 72], Chap. 1, Thm. 3). Die stetige Funktion

$$f : G \times G \longrightarrow E : (\sigma, \tau) \longmapsto f_{\sigma,\tau} := u_\sigma u_\tau u_{\sigma\tau}^{-1} \qquad (2.9)$$

ist wegen $\pi(f_{\sigma,\tau}) = 1$ für alle $\sigma, \tau \in G$ und $d_2 f = 1$ bereits ein 2-Kozykel von G mit Koeffizienten in A (hier multiplikativ aufgefaßt). f ist bis auf kohomologische Äquivalenz unabhängig von der Wahl des Repräsentanten aus $[(*)]$ und der Wahl von u.

Die Umkehrabbildung wird wie folgt konstruiert: Ist $f \in \mathrm{Z}^2(G, A)$ gegeben, so ist $E := A \times G$ mit der Multiplikation

$$(a, \sigma)\,(b, \tau) := (ab^{\sigma} f_{\sigma,\tau}, \sigma\tau) \tag{2.10}$$

eine Gruppe, deren Einselement $(f_{1,1}^{-1}, 1)$ ist. Die Homomorphismen $i : \ A \to E : a \mapsto (f_{1,1}^{-1} a, 1)$ und $\pi : E \to G : \ (a, \sigma) \mapsto \sigma$ induzieren eine Gruppenerweiterung

$$1 \longrightarrow A \ \xrightarrow{\ i\ }\ E \ \xrightarrow{\ \pi\ }\ G \longrightarrow 1.$$

Ein anderer Repräsentant aus (f) führt zu einer isomorphen Erweiterung. □

In diesem Sinn spricht man also von einem 2-Kozykel f, der zu einer Gruppenerweiterung $(*)$ korrespondiert, oder umgekehrt. Die Isomorphieklasse einer *zerfallenden Gruppenerweiterung* $(*)$, d.h. der zu $(*)$ gehörende stetige Schnitt u ist bereits ein Homomorphismus, wird unter der Bijektion aus Satz 2.4 auf das Einselement $\mathrm{B}^2(G, A)$ aus $\mathrm{H}^2(G, A)$ abgebildet.

Daß es tatsächlich sinnvoll war, die Kohomologie für proendliche Gruppen einzuführen, zeigt das folgende Lösbarkeitskriterium von HOECHSMANN für ein Einbettungsproblem der Form (2.8). Vermöge φ operiert $\mathcal{G}$ ebenfalls auf A: $a^{\sigma} := a^{\varphi(\sigma)}$ für alle $a \in A, \sigma \in \mathcal{G}$. Für den Kern $\mathcal{G}_0$ von φ, welcher ein abgeschlossener Normalteiler von $\mathcal{G}$ ist, gilt $\mathcal{G}/\mathcal{G}_0 \cong G$ und $A^{\mathcal{G}_0} = A$. Sei $\inf = \inf_{\mathcal{G}}^{G}$ die Inflationsabbildung aus (2.3).

Satz 2.5 (Hoechsmann)

Sei $(f) \in \mathrm{H}^2(G, A)$ die zu $[(*)]$ korrespondierende 2-Kozykelklasse. Das Einbettungsproblem $\mathcal{E}(\mathcal{G}, \varphi, (*))$ aus (2.8) ist genau dann lösbar, wenn $\inf((f)) = 1 \in \mathrm{H}^2(\mathcal{G}, A)$ ist.

Beweis:

Es bezeichne $E \times_G \mathcal{G} := \{(e, \sigma) \in E \times \mathcal{G} \mid \pi(e) = \varphi(\sigma)\}$ das *Faserprodukt* von E und $\mathcal{G}$ über G. In dem Diagramm

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & A & \xrightarrow{\hat{i}} & E \times_G \mathcal{G} & \xrightarrow{\mathrm{pr}_2} & \mathcal{G} & \longrightarrow & 1 \qquad (**) \\
 & & & & \Big\downarrow{\scriptstyle \mathrm{pr}_1} & \swarrow{\scriptstyle \psi} & \Big\downarrow{\scriptstyle \varphi} & & \\
1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \qquad (*)
\end{array}
\tag{2.11}
$$

mit den natürlichen Projektionen $\mathrm{pr}_1, \mathrm{pr}_2$ und $\hat{i}(a) := (i(a), 1_{\mathcal{G}})$ ist die obere exakte Sequenz $(**)$ eine Gruppenerweiterung von $\mathcal{G}$ mit abelschem Kern A, zu der die 2-Kozykelklasse $\inf((f)) \in \mathrm{H}^2(\mathcal{G}, A)$ gehört. Die Lösbarkeit des Einbettungsproblems (2.8) ist also gleichwertig mit dem Zerfall von $(**)$ in (2.11), was gerade $\inf((f)) = 1 \in \mathrm{H}^2(\mathcal{G}, A)$ bedeutet. (Siehe [Hoe 68], Abschnitt 1.1.) □

2.3 Die Brauergruppe

Sei k ein Körper. Eine k-Algebra A ist *zentral-einfach*, wenn A einfach, zentral und endlichdimensional über k ist. Die *Brauergruppe* $\mathrm{Br}(k)$ von k besteht aus den Ähnlichkeitsklassen $[A]$ zentral-einfacher k-Algebren A. Dabei heißen zwei zentral-einfache k-Algebren A, B *ähnlich* (in Zeichen: $A \sim B$), wenn es $r, s \in \mathbb{N}$ mit

$$A \otimes_k \mathrm{M}_r(k) \cong B \otimes_k \mathrm{M}_s(k)$$

gibt, wobei $\mathrm{M}_r(k)$ den Ring der $r \times r$-Matrizen mit Koeffizienten aus k bezeichnet. Die auf dem Tensorprodukt basierende Verknüpfung

$$[A]\,[B] := [A \otimes_k B]$$

macht $\mathrm{Br}(k)$ zu einer abelschen Gruppe. Ist K/k eine Körpererweiterung, so heißt der Kern der *(algebrentheoretischen) Restriktion*

$$\mathrm{res}_{K/k} \;:\; \mathrm{Br}(k) \longrightarrow \mathrm{Br}(K) \;:\; [A] \longmapsto [A \otimes_k K] \tag{2.12}$$

die *relative Brauergruppe* $\mathrm{Br}(K/k)$ von k bezüglich K. Für zentral-einfache k-Algebren aus $[A] \in \mathrm{Br}(K/k)$ ist K ein *Zerfällungskörper*. Es gilt $\mathrm{Br}(k) = \bigcup_K \mathrm{Br}(K/k)$, wobei K die endlichen Galoiserweiterungen von k in $\overline{k}$ durchläuft.

Sei K/k eine endliche Galoiserweiterung vom Grad $n = (K : k)$ mit Galoisgruppe $G = \mathrm{G}(K/k)$. Sei $f : G \times G \to K^\times$ ein 2-Kozykel. Das *verschränkte Produkt* von K und G bezüglich f ist der n^2-dimensionale k-Vektorraum

$$(K, G, f) := \bigoplus_{\sigma \in G} K\, u_\sigma$$

mit formalen Symbolen u_σ, auf dem man eine Multiplikation

$$(\sum_{\sigma \in G} \alpha_\sigma u_\sigma)(\sum_{\tau \in G} \beta_\tau u_\tau) := \sum_{\sigma,\tau \in G} \alpha_\sigma \beta_\tau^\sigma f_{\sigma,\tau} u_{\sigma\tau} \qquad (\alpha_\sigma, \beta_\tau \in K)$$

definiert. (K, G, f) ist eine zentral-einfache k-Algebra, die über K zerfällt (siehe [Ker 90], Kap. III, Satz 13.4). Die Konstruktion des verschränkten Produktes legt das Fundament für den folgenden

Satz 2.6

Sei K/k eine endliche Galoiserweiterung mit $G = \mathrm{G}(K/k)$. Dann ist die Abbildung

$$\mathrm{H}^2(G, K^\times) \xrightarrow{\cong} \mathrm{Br}(K/k) \ : \ (f) \longmapsto [(K, G, f)]$$

ein Gruppenisomorphismus. Ist $\mathcal{G} = \mathrm{G}(\overline{k}/k)$ die absolute Galoisgruppe von k, so folgt durch den Übergang zum induktiven Limes

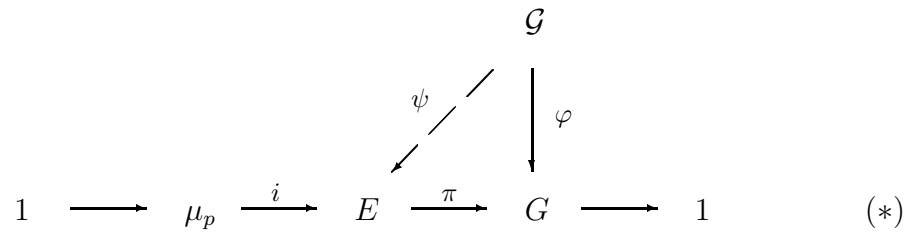
$$\mathrm{H}^2(\mathcal{G}, \overline{k}^\times) \cong \mathrm{Br}(k).$$

Beweis:

Siehe [Ker 90], Kap. III, Thm. 14.3; [Lor 90], §30*, Bemerkung zu F4. □

Unter bestimmten Voraussetzungen kann man die Lösbarkeit eines Einbettungsproblems an dem Zerfall einer gewissen zentral-einfachen k-Algebra festmachen. Sei dazu k ein algebraischer Zahlkörper, der die Gruppe μ_p der p-ten Einheitswurzeln für ein $p \in \mathbb{N}$ enthalte. Sei K/k eine endliche Galoiserweiterung mit $G = \mathrm{G}(K/k)$. Dann operiert G trivial auf $A = \mu_p$. In dem zentralen Einbettungsproblem

(2.13)



für eine endliche Gruppe E gehe $f \in \mathrm{Z}^2(G, \mu_p)$ im Sinne von Satz 2.4 mit $(*)$ einher.

Satz 2.7

Das zentrale Einbettungsproblem $\mathcal{E}(\mathcal{G}, \varphi, (*))$ aus (2.13) ist genau dann lösbar, wenn das verschränkte Produkt (K, G, f) bereits über k zerfällt.

Beweis:

Der Homomorphismus in der unteren Zeile des kommutativen Diagrammes

(2.14)

$$\begin{array}{ccccc} \mathrm{H}^2(G, \mu_p) & \longrightarrow & \mathrm{H}^2(G, K^\times) & \cong & \mathrm{Br}(K/k) \\ \downarrow \text{inf} & & \uparrow \text{inf} & & \uparrow \\ \mathrm{H}^2(\mathcal{G}, \mu_p) & \hookrightarrow & \mathrm{H}^2(\mathcal{G}, \overline{k}^\times) & \cong & \mathrm{Br}(k). \end{array}$$

stammt aus der langen exakten Kohomologiesequenz, die durch die exakte *Kummer-Sequenz*

$$1 \longmapsto \mu_p \longrightarrow \overline{k}^\times \xrightarrow{p} \overline{k}^\times \longrightarrow 1$$

induziert wird, wobei die Abbildung p für das Potenzieren $x \mapsto x^p$ steht. Seine Injektivität folgt aus Gleichung (2.4) (Hilbert 90). Es gilt:

$$\begin{aligned} \mathcal{E}(\mathcal{G}, \varphi, (*)) \quad \text{ist lösbar} &\iff \mathrm{inf}((f)) = 1 \in \mathrm{H}^2(\mathcal{G}, \mu_p) \\ &\iff \mathrm{inf}((f)) = 1 \in \mathrm{H}^2(\mathcal{G}, \overline{k}^\times) \\ &\iff [A_{\mathrm{inf}((f))}] = 1 \in \mathrm{Br}(k), \end{aligned}$$

wobei $A_{\mathrm{inf}((f))}$ eine zentral-einfache k-Algebra sei, die das Bild von $\mathrm{inf}((f))$ unter dem Isomorphismus $\mathrm{H}^2(\mathcal{G}, \overline{k}^\times) \xrightarrow{\cong} \mathrm{Br}(k)$ repräsentiert. Andererseits wird $(f) \in \mathrm{H}^2(G, \mu_p)$

auf $[(K,G,f)] \in \mathrm{Br}(K/k) \leq \mathrm{Br}(k)$ abgebildet, so daß aufgrund der Kommutativität von (2.14)

$$A_{\inf((f))} \sim (K,G,f)$$

ist. Somit gilt:

$$\mathcal{E}(\mathcal{G},\varphi,(*)) \quad \text{ist lösbar} \iff [(K,G,f)] = 1 \in \mathrm{Br}(k),$$
$$\text{d.h. } (K,G,f) \text{ zerfällt bereits über } k. \quad \square$$

2.4 Ergebnisse der Diplomarbeit

Im Fall eines zentralen Einbettungsproblems der Form (2.13) kann man folgende Existenzaussage treffen: Zu der dem *Hindernis* $\inf((f)) \in \mathrm{H}^2(\mathcal{G},\mu_p)$ entsprechenden Algebrenklasse $[A] \in \mathrm{Br}(k)_p$ existieren $a,b \in k^\times$ mit $A_{\zeta_p}(a,b) \sim A$; dabei ist

$$A_{\zeta_p}(a,b) := \bigoplus_{i,j=0}^{p-1} k u^i v^j \qquad \text{mit} \qquad u^p = a,\ v^p = b,\ vu = \zeta_p uv$$

die *Normrestalgebra* zu a,b und einer primitiven p-ten Einheitswurzel ζ_p, die bereits im Zahlkörper k liegt. u,v sind formale Symbole, die den obigen Relationen gehorchen. $A_{\zeta_p}(a,b)$ zerfällt genau dann über k, wenn b eine Norm in $k(\sqrt[p]{a})$ ist (siehe [Ker 90], Kap. IV, Satz 17.4).

Das folgende Ergebnis benutzt zum einen den Satz von Albert-Hasse-Brauer-Noether, der ein Lokal-Global-Prinzip für zentral-einfache k-Algebren über einem algebraischen Zahlkörper k beschreibt: Eine zentral-einfache k-Algebra zerfällt genau dann über k, wenn sie überall lokal, d.h. über allen Komplettierungen $k_\mathfrak{p}$, zerfällt. Zum anderen fließt der Satz von Grunwald-Hasse-Wang ein, der im wesentlichen besagt, daß – bis auf einen Ausnahmefall, den sogenannten *speziellen Fall* – für eine endliche Primstellenmenge S und vorgegebene Galoiserweiterungen $K_\mathfrak{p}/k_\mathfrak{p}$ $(\mathfrak{p} \in S)$ stets eine globale Erweiterung K/k existiert, deren Komplettierung bezüglich aller $\mathfrak{p} \in S$ gerade der vorgegebene Körper $K_\mathfrak{p}$ ist.

Satz 2.8

Sei $\mathcal{E}$ ein zentrales Einbettungsproblem wie in (2.13) über einem algebraischen Zahlkörper k mit $\mu_p \subseteq k$. Dann gibt es ein zentrales Einbettungsproblem $\tilde{\mathcal{E}}$, zu dessen Hindernis $\inf((\tilde{f}))$ die Normrestalgebra $A_{\zeta_p}(a,b)$ mit $a,b \in k^\times$ gehört, so daß gilt:

$$\mathcal{E} \text{ ist lösbar} \iff \tilde{\mathcal{E}} \text{ ist lösbar}$$
$$\iff b \text{ ist eine Norm in } k(\sqrt[p]{a})/k.$$

Beweis:

Siehe [Som 96], Satz 8.10. □

Wie man hier im allgemeinen zu konkreten Normkriterien kommt, ist allerdings unklar. Lediglich im Fall einer zyklischen Gruppe G ist dies bekannt, da es für den Zerfall einer zyklischen Algebra stets ein Normkriterium gibt (siehe [Som 96], Kap. 7, Satz 7.3 und Kor. 7.4). Mit der Fragestellung, ob es derartige Lösbarkeitskriterien in Form von Normgleichungen auch im (nicht-zyklischen) abelschen Fall gibt, habe ich mich im Rahmen meiner Diplomarbeit [Som 96] befaßt, in der ich für zentrale Einbettungsprobleme Lösbarkeitskriterien suchte. Ein Beispiel daraus, auf das im Verlauf dieser Arbeit noch zurückgekommen wird, möge die Dinge verdeutlichen.

Sei $k = \mathbb{Q}$ und $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ mit $a, b \in \mathbb{Q}^\times$, derart daß $G = \mathrm{G}(K/k)$ isomorph zur Kleinschen Vierergruppe $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist. Sei $\mathcal{G} = \mathrm{G}(\overline{\mathbb{Q}}/\mathbb{Q})$ die absolute Galoisgruppe von $\mathbb{Q}$. Es sei $p = 2$, d.h. $\zeta_2 = -1$. Die Normrestalgebra $A_{-1}(a, b)$ wird kurz (a, b) geschrieben und *Quaternionenalgebra* genannt. Es bezeichne D_4 die *Diedergruppe* der Ordnung 8. Dann läßt sich die Frage, ob das zentrale Einbettungsproblem

(2.15)
$$\begin{array}{ccccccccc} & & & & & & \mathcal{G} & & \\ & & & & & \overset{\psi}{\swarrow} & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & D_4 & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array} \qquad (*)$$

eine Lösung besitzt, darauf zurückführen, ob die Normgleichung $\mathrm{N}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(x + y\sqrt{a}) = b$, d.h.

(2.16) $$x^2 - ay^2 = b$$

für gewisse $x, y \in \mathbb{Q}$ lösbar ist. Abschließend sei bemerkt, daß die Rollen von a und b natürlich vertauschbar sind: Ist (2.16) lösbar, so ist auch

$$x'^2 - by'^2 = a \tag{2.17}$$

mit $x' = xy^{-1}$ und $y' = y^{-1}$ lösbar und umgekehrt; dabei ist $y \neq 0$, sonst wäre $x^2 = b$ und damit $\sqrt{b} \in \mathbb{Q}$.

Zu der Gruppenerweiterung $(*)$ gehört der folgende 2-Kozykel $f : G \times G \to \mu_2$:

(2.18)

$f_{\rho,\eta}$	id	σ	τ	$\sigma\tau$
id	1	1	1	1
σ	1	1	-1	-1
τ	1	1	1	1
$\sigma\tau$	1	1	-1	-1

Dabei durchläuft ρ die Zeilen und η die Spalten; es ist etwa $f_{\sigma,\tau} = -1$, während $f_{\tau,\sigma} = 1$ ist.

Siehe auch [Som 96], Kap. 8, Bsp. 3.

Kapitel 3

Brauerkörper

In diesem Kapitel wird basierend auf einer Arbeit von ROQUETTE ([Roq 63]) die Konstruktion eines gewissen Funktionenkörpers beschrieben. Dieser sogenannte Brauerkörper ist Zerfällungskörper einer zentral-einfachen k-Algebra, die durch einen 2-Kozykel über die Bildung des verschränkten Produkts gewonnen wird. Im Hinblick auf ein gegebenes zentrales Einbettungsproblem, bei dem dieser 2-Kozykel zu der Gruppenerweiterung korrespondiert, erhält man also in Form des Brauerkörpers einen virtuellen Grundkörper, über dem das Einbettungsproblem lösbar ist.

3.1 Gruppentheoretische Betrachtungen

Sei G eine (endliche) Gruppe. Vorgelegt sei eine kurze exakte Sequenz

$$1 \longrightarrow C \longrightarrow A \longrightarrow B \longrightarrow 1 \tag{3.1}$$

von (nicht notwendigerweise abelschen) Gruppen mit G-Operation, stets als Potenz geschrieben. Dabei liege C im Zentrum von A. Dies induziert eine im Sinne der nicht-abelschen Kohomologie exakte Sequenz

$$\mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(G, B) \longrightarrow \mathrm{H}^2(G, C). \tag{3.2}$$

Die *zerfallende Erweiterung* $\overline{A} := \{a\sigma \mid a \in A,\ \sigma \in G\}$ von A mit G (oder auch das *semidirekte Produkt* von A und G bezüglich der betrachteten Operation von G auf A) ist mit der Verknüpfung

$$(a\sigma)\,(a'\tau) := (aa'^{\sigma})(\sigma\tau) \qquad (a, a' \in A,\ \sigma, \tau \in G) \tag{3.3}$$

eine Gruppe, die A – identifiziert mit $A\,1_G$ – als Normalteiler und G – identifiziert mit $1_A\,G$ – als Untergruppe enthält. Es ist (als Mengen)

$$G \cap A = 1 \qquad \text{und} \qquad AG = \overline{A}. \tag{3.4}$$

Die 1-Kozykelklassen[1] $(b_\sigma) \in \mathrm{H}^1(G, B)$ liefern eine Beschreibung einer gewissen Klasse von Untergruppen von $\overline{A}$. Sind nämlich $a_\sigma \in A$ Urbilder der b_σ, so ist $U := \{ca_\sigma\sigma \mid c \in C,\, \sigma \in G\}$ eine Untergruppe von $\overline{A}$ mit den Eigenschaften

$$U \cap A = C \qquad \text{und} \qquad AU = \overline{A}, \tag{3.5}$$

deren Faktorgruppe U/C natürlich isomorph zu $\overline{A}/A \cong G$ ist. Ist umgekehrt eine Untergruppe $U \leq \overline{A}$ mit den Eigenschaften (3.5) gegeben, so kann man zu jedem $\sigma \in G$ ein modulo C eindeutig bestimmtes $u_\sigma \in U$ mit $u_\sigma \equiv \sigma \bmod A$ finden. Zu jedem dieser u_σ wiederum gibt es ein modulo C eindeutig bestimmtes $a_\sigma \in A$ mit $u_\sigma = a_\sigma\sigma$, so daß die Bilder b_σ der a_σ in B wegen $B \cong A/C$ eindeutig bestimmt sind. Die 1-Kozykel-Eigenschaft der b_σ folgt sofort aus (3.3).

Zwei Untergruppen U, U' mit den Eigenschaften (3.5) sind wegen

$$a(a_\sigma\sigma)a^{-1} = (aa_\sigma a^{-\sigma})\sigma \qquad (a \in A, \sigma \in G)$$

genau dann *A-konjugiert* zueinander, d.h. $aUa^{-1} = U'$ für ein $a \in A$, wenn für die entsprechenden 1-Kozykel b_σ, b'_σ

$$b'_\sigma = bb_\sigma b^{-\sigma} = (b^{-1})^{-1} b_\sigma (b^{-1})^\sigma \qquad (\sigma \in G)$$

kohomologische Äquivalenz vorliegt (siehe (2.6)), wobei $b \in B$ das Bild von a sei.

Jede Untergruppe U mit (3.5) definiert zugleich eine Gruppenerweiterung von G mit C und somit einen 2-Kozykel

$$c_{\sigma,\tau} := u_\sigma u_\tau u_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G) \tag{3.6}$$

von G mit Werten in C, wobei u_σ (analog $u_\tau, u_{\sigma\tau}$) ein Urbild von $\sigma \in G$ unter $U \to G$ ist. Zwei Untergruppen U, U' mit (3.5) sind *von demselben Erweiterungstyp*,

[1] In diesem Kapitel bezeichne $(f_{\sigma_1,\ldots,\sigma_n})$ stets eine n-Kozykelklasse und $f_{\sigma_1,\ldots,\sigma_n}$ die Werte in dem jeweiligen G-Modul bzw. der jeweiligen G-Gruppe.

wenn ihre entsprechenden 2-Kozykeln $c_{\sigma,\tau}, c'_{\sigma,\tau}$ kohomolog sind. Schreibt man u_σ wieder in der Form $a_\sigma\sigma$ für ein $a_\sigma \in A$, so folgt aus $(a_\sigma\sigma)\,(a_\tau\tau) = c_{\sigma,\tau}(a_{\sigma\tau}\sigma\tau)$ nach (3.3)

$$c_{\sigma,\tau} = a_\sigma a_\tau^\sigma a_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G), \tag{3.7}$$

d.h. $(c_{\sigma,\tau}) \in \mathrm{H}^2(G, C)$ ist das Bild von $(b_\sigma) \in \mathrm{H}^1(G, B)$. Bewiesen ist somit:

Feststellung 3.1

Deutet man die 1-Kozykelklassen $(b_\sigma) \in \mathrm{H}^1(G, B)$ als die Klassen von A-konjugierten Untergruppen $U \leq \overline{A}$ mit den Eigenschaften

$$U \cap A = C \qquad \text{und} \qquad AU = \overline{A}$$

und deutet man die 2-Kozykelklassen $(c_{\sigma,\tau}) \in \mathrm{H}^2(G, C)$ als die Erweiterungstypen dieser U (als Gruppenerweiterungen von G mit C), so ordnet die Abbildung $\mathrm{H}^1(G, B) \to \mathrm{H}^2(G, C)$ jeder A-Konjugationsklasse von Untergruppen U den entsprechenden Erweiterungstyp zu, d.h.

$$(b_\sigma) \longmapsto (c_{\sigma,\tau}). \qquad \square$$

Das Bild von $\mathrm{H}^1(G, B) \to \mathrm{H}^2(G, C)$ besteht also aus genau denjenigen 2-Kozykelklassen, deren Erweiterungstyp durch eine Untergruppe $U \leq \overline{A}$ mit (3.5) realisiert werden kann.

Korollar 3.2

Die Abbildung $\mathrm{H}^1(G, B) \to \mathrm{H}^2(G, C)$ ist genau dann injektiv, wenn zwei beliebige Untergruppen, die die Bedingungen (3.5) erfüllen und zugleich denselben Erweiterungstyp haben, stets A-konjugiert sind. $\square$

3.2 Die Abbildung $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \longrightarrow \mathrm{H}^2(G, K^\times)$

Es sei G die Galoisgruppe $\mathrm{G}(K/k)$ einer endlichen Erweiterung K/k vom Grad $n = (K : k)$. Sei $m \in \mathbb{N}$. Man setze nun

$$C = K^\times, \qquad A = \mathrm{GL}_m(K) \qquad \text{und} \qquad B = \mathrm{PGL}_m(K).$$

Dabei ist $\mathrm{PGL}_m(K) = \mathrm{GL}_m(K)/K^\times$ die *projektive lineare Gruppe* von K, deren G-Operation durch die koeffizientenweise Operation von G auf die Matrizen aus $\mathrm{GL}_m(K)$ induziert wird. Die kurze exakte Sequenz

$$1 \longrightarrow K^\times \longrightarrow \mathrm{GL}_m(K) \longrightarrow \mathrm{PGL}_m(K) \longrightarrow 1 \tag{3.8}$$

induziert eine lange exakte Kohomologiesequenz

$$1 \overset{(2.7)}{=} \mathrm{H}^1(G, \mathrm{GL}_m(K)) \longrightarrow \mathrm{H}^1(G, \mathrm{PGL}_m(K)) \overset{\Delta^2}{\longrightarrow} \mathrm{H}^2(G, K^\times) \tag{3.9}$$

im Sinne der nicht-abelschen Kohomologie.

Zunächst soll die zerfallende Erweiterung $\overline{\mathrm{GL}_m(K)}$ von $\mathrm{GL}_m(K)$ mit G als eine Untergruppe des Endomorphismenringes eines K-Vektorraums charakterisiert werden. Sei dazu V ein K-Vektorraum der Dimension m mit K-Basis $v_1, \ldots, v_m$. Eine Matrix $a = (a_{ij})_{i,j=1,\ldots,m} \in \mathrm{GL}_m(K)$ ist wie üblich durch lineares Fortsetzen von

$$a \ : \ v_j \longmapsto \sum_{i=1}^{m} a_{ij} v_i \qquad (j = 1, \ldots, m) \tag{3.10}$$

eine K-lineare Abbildung. Auf diese Weise identifiziert man $\mathrm{GL}_m(K)$ mit der Gruppe aller K-Automorphismen von V. Betrachtet man V als k-Vektorraum, so daß V von den Elementen $cv_j,\ c \in K$ aufgespannt wird, so ist $\mathrm{GL}_m(K)$ eine Untergruppe des Ringes $\mathrm{End}_k(V)$ aller k-Endomorphismen von V.

G läßt sich ebenfalls als Untergruppe von $\mathrm{End}_k(V)$ auffassen, indem man ein $\sigma \in G$ als die lineare Fortsetzung von

$$\sigma \ : \ c\, v_j \longmapsto c^\sigma v_j \qquad (c \in K, j = 1, \ldots, m) \tag{3.11}$$

auf V begreift. Somit gilt in $\mathrm{End}_k(V)$

$$\sigma a \sigma^{-1} = a^\sigma \qquad (\sigma \in G, a \in \mathrm{GL}_m(K)). \tag{3.12}$$

Da kein $\sigma \in G, \sigma \neq \mathrm{id}$ K-linear ist, folgt $G \cap \mathrm{GL}_m(K) = 1$, so daß insgesamt bewiesen ist:

Lemma 3.3

Sei V ein K-Vektorraum der Dimension m. Dann ist die zerfallende Erweiterung $\overline{\mathrm{GL}_m(K)}$ von $\mathrm{GL}_m(K)$ mit G identifizierbar mit einer Untergruppe des Ringes

$\mathrm{End}_k(V)$ der k-Endomorphismen von V derart, daß $\mathrm{GL}_m(K)$ die volle Gruppe der K-Automorphismen von V ist. □

Um die Abbildung $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ zu untersuchen, muß man die Untergruppen

$$U \leq \overline{\mathrm{GL}_m(K)}$$

studieren, die den Relationen (3.5)

$$U \cap \mathrm{GL}_m(K) = K^\times \qquad \text{und} \qquad \mathrm{GL}_m(K)\, U = \overline{\mathrm{GL}_m(K)} \tag{3.13}$$

genügen. Mit Blick auf (3.6) und (3.12) erkennt man die Struktur des von U erzeugten Teilringes $[U]$ in $\mathrm{End}_k(V)$:

$$u_\sigma\, u_\tau = c_{\sigma,\tau}\, u_{\sigma\tau} \qquad \text{und} \qquad u_\sigma\, c = c^\sigma\, u_\sigma \qquad\qquad (c \in K,\ \sigma, \tau \in G). \tag{3.14}$$

$[U]$ ist also gerade das verschränkte Produkt $(K, G, c_{\sigma,\tau})$, wobei die Klasse des 2-Kozykels $c_{\sigma,\tau}$ in $\mathrm{H}^2(G, K^\times)$ den Erweiterungstyp von U als Gruppenerweiterung von G mit $K^\times$ bestimmt.

Der von U' erzeugte Teilring $[U']$ einer Untergruppe U', die (3.13) erfüllt und von demselben Erweiterungstyp wie U ist (d.h. der entsprechende 2-Kozykel $c'_{\sigma,\tau}$ ist kohomolog zu $c_{\sigma,\tau}$) ist isomorph zu $[U]$. Nach dem Satz von Skolem-Noether (siehe [Ker 90], Kap. II, Satz 8.2) wird dieser Isomorphismus $\Phi : [U] \to [U']$ durch einen inneren Automorphismus aus $\mathrm{End}_k(V)$ gegeben, d.h. es gibt ein $a \in \mathrm{End}_k(V)$ mit $\Phi(u) = aua^{-1}$. Da a invertierbar ist, liegt a nach Lemma 3.3 in $\mathrm{GL}_m(K)$. Weil Φ U in U' überführt, gilt:

Feststellung 3.4

Sind U, U' zwei Untergruppen von $\overline{\mathrm{GL}_m(K)}$ mit (3.13) und von demselben Erweiterungstyp $(c_{\sigma,\tau}) \in \mathrm{H}^2(G, K^\times)$, so sind sie $\mathrm{GL}_m(K)$-konjugiert. □

Aus Korollar 3.2 folgt:

Korollar 3.5

Die Abbildung $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ ist injektiv. □

Zum Abschluß dieses Abschnittes wird noch das Bild von $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ bestimmt. Ein beliebiges Element $(c_{\sigma,\tau}) \in \mathrm{H}^2(G, K^\times)$ liegt nämlich genau dann im Bild, wenn es zu dem verschränkten Produkt $(K, G, c_{\sigma,\tau})$ einen Darstellungsmodul V der K-Dimension m gibt. Letzteres bedeutet, daß es einen K-Vektorraum V mit $\dim_K V = m$ derart gibt, daß man $(K, G, c_{\sigma,\tau})$ als Teilring von $\mathrm{End}_k(V)$ realisieren kann. Mit anderen Worten: V ist ein $(K, G, c_{\sigma,\tau})$-Modul.

Sei A eine zentral-einfache k-Algebra und D der bis auf k-Isomorphie eindeutig bestimmte Schiefkörper mit Zentrum k und $A \sim D$. Man definiert den *Schurindex* von A als

$$\mathrm{s}(A) := \mathrm{s}([A]) := \sqrt{\dim_k D}.$$

Dieser ist stets ein Teiler des *(reduzierten) Grades* $\sqrt{\dim_k A}$ von A und genau dann gleich dem Grad von A, wenn A ein Schiefkörper ist. Der Schurindex eines 2-Kozykels $c_{\sigma,\tau}$ von G mit Werten in $K^\times$ ist durch den Schurindex des zugehörigen verschränkten Produktes erklärt:

$$\mathrm{s}(c_{\sigma,\tau}) := \mathrm{s}((K, G, c_{\sigma,\tau})).$$

Nun gibt es zu $(K, G, c_{\sigma,\tau})$ genau dann einen Darstellungsmodul der K-Dimension m, wenn $\mathrm{s}(c_{\sigma,\tau})$ ein Teiler von m ist ([Roq 63], §3, Prop. 5). Somit gilt:

Satz 3.6

Ein Element $(c_{\sigma,\tau}) \in \mathrm{H}^2(G, K^\times)$ ist genau dann im Bild der injektiven Abbildung $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ enthalten, wenn sein Schurindex $\mathrm{s}(c_{\sigma,\tau})$ ein Teiler von m ist. □

In [Roq 63] wird aber kein effektives Verfahren zur Bestimmung eines Urbildes – wenn es denn existiert – angegeben. Wie man später sehen wird (siehe Beweis von Satz 3.16), ist dies aber nötig und beruht auf der folgenden Überlegung.

Der Schurindex einer zentral-einfachen Algebra ist stets Teiler des Grades eines Zerfällungskörpers der Algebra über dem Grundkörper, sofern der Grad endlich ist (siehe [Lor 90], §29, Satz 19). Da K Zerfällungskörper für jedes Element aus $H^2(G, K^\times) \cong \mathrm{Br}(K/k)$ ist, gilt:

Korollar 3.7

Sei m ein Vielfaches von $n = (K : k)$. Dann ist $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ eine Bijektion. □

Man kann also zu jedem beliebigen $(c_{\sigma,\tau}) \in \mathrm{H}^2(G, K^\times)$ stets ein m finden, so daß es ein $(b_\sigma) \in \mathrm{H}^1(G, \mathrm{PGL}_m(K))$ mit

$$c_{\sigma,\tau} = b_\sigma b_\tau^\sigma b_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G)$$

gibt. Solch ein m ist im allgemeinen zwar nicht minimal, aber es hat den Vorteil, daß man explizit Elemente $a_\sigma \in GL_m(K)$ berechnen kann, für die

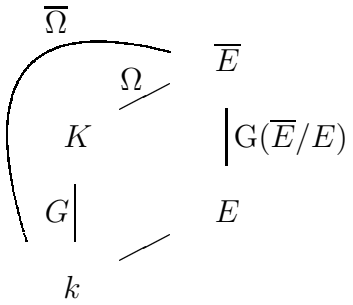
$$c_{\sigma,\tau} = a_\sigma a_\tau^\sigma a_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G)$$

gilt und deren Bilder b_σ in $\mathrm{PGL}_m(K)$ die 1-Kozykelklasse (b_σ) mit $(b_\sigma) \mapsto (c_{\sigma,\tau})$ definieren. Die Konstruktion dieser a_σ wird in Abschnitt 4.1 erläutert.

3.3 Galoistheoretische Anwendung

In diesem Abschnitt werden die gruppentheoretischen Betrachtungen aus Abschnitt 3.1 im Sinne der Galoistheorie gedeutet. Es sei

K/k	eine endliche Galoiserweiterung;
$n = (K : k)$	der Grad von K/k;
$G = \mathrm{G}(K/k)$	die Galoisgruppe von K/k;
E/k	eine beliebige, zu K linear disjunkte Erweiterung;
$\overline{E} = EK$	das körpertheoretische Kompositum von E und K (in einem fest gewählten algebraischen Abschluß);
$\mathrm{G}(\overline{E}/E) \cong G$	die – nach dem Translationssatz der Galoistheorie – zu G isomorphe Galoisgruppe von $\overline{E}/E$;
Ω	die Automorphismengruppe von $\overline{E}/K$;
$\overline{\Omega}$	die Automorphismengruppe von $\overline{E}/k$.



G operiert auf Ω wegen $\sigma\Omega\sigma^{-1} = \Omega$ durch Konjugation $\omega^\sigma := \sigma\omega\sigma^{-1}$ für $\sigma \in G$, $\omega \in \Omega$. Jedes $\overline{\omega} \in \overline{\Omega}$ induziert durch Einschränkung auf K ein $\sigma \in G$. Da $\omega := \overline{\omega}\sigma^{-1}$ K fix läßt und somit in Ω liegt, ist $\overline{\omega} = \omega\sigma \in \Omega G$. Wegen $\Omega \cap G = 1$ gilt:

Feststellung 3.8

Die Automorphismengruppe $\overline{\Omega}$ von $\overline{E}/k$ ist gerade die zerfallende Erweiterung $\overline{\Omega} = \Omega G$ von Ω mit G. □

Von Interesse sind nun die Teilkörper $F \subseteq \overline{E}$ mit

$$FK = \overline{E} \qquad \text{und} \qquad F \cap K = k. \tag{3.15}$$

Die Galoisgruppe $H := \mathrm{G}(\overline{E}/F)$ ist nach dem Translationssatz isomorph zu $\mathrm{G}(K/(F \cap K)) = \mathrm{G}(K/k) = G$, d.h. es ist $\Omega H/\Omega = \Omega G/\Omega$, also $\Omega H = \Omega G$. Somit ist

$$\Omega \cap H = 1 \qquad \text{und} \qquad \Omega H = \overline{\Omega}. \tag{3.16}$$

Ist umgekehrt H eine Untergruppe von $\overline{\Omega}$, die den Bedingungen (3.16) genügt, so ist $H \cong \overline{\Omega}/\Omega = G$ und damit endlich. Bezeichnet F den Fixkörper von $\overline{E}$ unter H, so folgt (3.15) für F aus (3.16) mittels der Galoistheorie.

Feststellung 3.9

Es gibt eine Bijektion zwischen den Teilkörpern $F \subseteq \overline{E}$ mit den Eigenschaften (3.15) und den Untergruppen $H \leq \overline{\Omega}$ mit den Eigenschaften (3.16), wobei $H = \mathrm{G}(\overline{E}/F)$ ist. □

Zwei Körper F, F' mit (3.15) sind über k linear disjunkt zu K, so daß jeder k-Isomorphismus $F \to F'$ in eindeutiger Weise zu einem K-Isomorphismus $\overline{E} =$

$FK \to \overline{E} = F'K$ erweitert werden kann. Letzterer wird aber durch ein Element $\omega \in \Omega$ induziert, d.h. $F' = F^\omega$, was aus galoistheoretischer Sicht gleichbedeutend mit $H' = \omega H \omega^{-1}$ ist:

Feststellung 3.10

Zwei Körper F, F' mit den Eigenschaften (3.15) sind genau dann k-isomorph, wenn ihre zugehörigen Galoisgruppen H, H' Ω-konjugiert sind. □

Aus den eben genannten Gründen wird jeder k-Automorphismus von F durch ein $\omega \in \Omega$ induziert, so daß man die Gruppe der k-Automorphismen von F als eine Untergruppe von Ω auffassen kann. $F = F^\omega$ ist gleichwertig mit $H = \omega H \omega^{-1}$.

Korollar 3.11

Die k-Automorphismengruppe eines Körpers F mit den Eigenschaften (3.15) ist natürlich isomorph zu dem Normalisator in Ω der F entsprechenden Untergruppe H von $\overline{\Omega}$. □

Wendet man die Ergebnisse aus Abschnitt 3.1 auf die exakte Sequenz

$$1 \longrightarrow 1 \longrightarrow \Omega \xrightarrow{\text{id}} \Omega \longrightarrow 1$$

an und ersetzt U durch H sowie b_σ durch ω_σ, so erhält man den folgenden

Satz 3.12

Es gibt eine Bijektion zwischen den Teilkörpern $F \subseteq \overline{E}$ mit den Eigenschaften

$$FK = \overline{E} \qquad \text{und} \qquad F \cap K = k$$

und den 1-Kozykeln ω_σ von G mit Werten in Ω. Korrespondieren F und ω_σ, so besteht die zugehörige Galoisgruppe $H = \mathrm{G}(\overline{E}/F)$ aus den Elementen $\omega_\sigma \sigma \in \overline{\Omega}$, $\sigma \in G$.

Zwei solche Körper F, F' sind genau dann k-isomorph, wenn ihre zugehörigen 1-Kozykeln $\omega_\sigma, \omega'_\sigma$ kohomolog sind, d.h. die k-Isomorphieklassen von Körpern mit o.g. Eigenschaften entsprechen bijektiv den 1-Kozykelklassen der Kohomologiemenge $\mathrm{H}^1(G, \Omega)$

Die Gruppe der k-Automorphismen eines solchen Körpers F ist natürlich isomorph zu der Untergruppe $\{\omega \in \Omega \mid \omega_\sigma = \omega \omega_\sigma \omega^{-\sigma} \ \ \forall\, \sigma \in G\}$. □

In der Anwendung dieser Theorie, die in den folgenden Abschnitten durchgeführt wird, wird lediglich eine gewisse G-invariante Untergruppe B von Ω gegeben sein,

so daß man die bisherigen Ergebnisse ein wenig verallgemeinern muß. Ein Körper F mit den Eigenschaften (3.15) heißt *B-zulässig*, wenn die Werte des zugehörigen 1-Kozykel ω_σ bereits in B liegen. Zwei Körper F, F' mit (3.15) werden *B-isomorph* genannt, wenn es einen Automorphismus $b \in B$ gibt, der F in F' überführt. Die *B-Automorphismengruppe* eines B-zulässigen Körpers F ist die Gruppe derjenigen Automorphismen von F, die durch ein Element b aus B induziert werden.

Die Satz 3.12 entsprechende Aussage lautet dann (siehe [Roq 63], §4, Prop. 6B):

Satz 3.13

Sei B eine G-invariante Untergruppe von Ω.

Dann gibt es eine Bijektion zwischen den B-zulässigen Teilkörpern $F \subseteq \overline{E}$ und den 1-Kozykeln b_σ von G mit Werten in B, wie sie in Satz 3.12 beschrieben ist, wobei man ω_σ dort durch b_σ ersetze. Die B-Isomorphieklassen von B-zulässigen Körpern entsprechen also bijektiv den 1-Kozykelklassen aus $\mathrm{H}^1(G, B)$.

Die B-Automorphismengruppe eines B-zulässigen Körpers F ist die Gruppe derjenigen Elemente $b \in B$, die $b_\sigma = b b_\sigma b^{-\sigma}$ für alle $\sigma \in G$ erfüllen. □

3.4 Der Brauerkörper einer zentral-einfachen Algebra

Es werde nun der spezielle Fall betrachtet, daß der Körper E der rationale Funktionenkörper

$$E = k(T) = k(T_1, \ldots, T_{m-1})$$

in $m-1$ Veränderlichen über k für ein $m \in \mathbb{N}$ ist. Dann ist

$$\overline{E} = EK = K(T) = K(T_1, \ldots, T_{m-1}).$$

$\mathrm{PGL}_m(K)$ operiert in der folgenden Weise als Automorphismengruppe auf $K(T)$: Sei S_m eine weitere Veränderliche. Man definiere S_j durch

$$S_j := T_j S_m, \qquad \text{d.h.} \qquad T_j = S_j S_m^{-1} \qquad (j = 1, \ldots, m-1) \tag{3.17}$$

und betrachte den Funktionenkörper $K(S) = K(S_1, \ldots, S_m)$ in m Veränderlichen, der $K(T)$ als Teilkörper enthält. Genauer: $K(T)$ ist die Menge der vom Grad 0 homogenen Elemente in $K(S)$. Ein $a = (a_{ij})_{i,j=1,\ldots,m} \in \mathrm{GL}_m(K)$ wird durch

$$S_j \longmapsto \sum_{i=1}^{m} a_{ij} S_i \qquad (j = 1, \ldots, m)$$

zu einem K-Automorphismus von $K(S)$, so daß $\mathrm{GL}_m(K)$ zu einer Automorphismengruppe von $K(S)$ wird. Aufgrund der Linearität werden homogene Elemente auf homogene Elemente abgebildet; insbesondere wird $K(T)$ also durch a in sich selbst überführt. a induziert genau dann die Identitätsabbildung, wenn es ein skalares Vielfaches $a = c \in K^\times$ der Einheitsmatrix ist. Somit wird die Faktorgruppe $\mathrm{PGL}_m(K) = \mathrm{GL}_m(K)/K^\times$ zu einer Automorphismengruppe von $K(T)$.

Beachtet man, daß G gemäß (3.11) trivial auf den S_j und koeffzientenweise auf den Elementen aus $\mathrm{GL}_m(K)$ operiert, so ist die im vorherigen Abschnitt definierte Operation von G auf $\mathrm{GL}_m(K)$ identisch mit der natürlichen Operation

$$a^\sigma = \sigma a \sigma^{-1} \qquad (a \in \mathrm{GL}_m(K), \sigma \in G).$$

Dies gilt in gleicher Weise für die Operation von G auf $\mathrm{PGL}_m(K)$. Insbesondere ist $\mathrm{PGL}_m(K)$ G-invariant und nimmt die Rolle der Untergruppe B in Satz 3.13 ein.

Sei nun eine 2-Kozykelklasse $\gamma = (c_{\sigma,\tau}) \in \mathrm{H}^2(G, K^\times)$ gegeben, deren Schurindex $\mathrm{s}(\gamma)$ ein Teiler von m ist. Nach Satz 3.6 ist γ das Bild einer eindeutig bestimmten 1-Kozykelklasse $\beta = (b_\sigma) \in \mathrm{H}^1(G, \mathrm{PGL}_m(K))$. Zu β gehört nach Satz 3.13 ein $\mathrm{PGL}_m(K)$-zulässiger Körper F mit

$$FK = K(T) \qquad \text{und} \qquad F \cap K = k, \tag{3.18}$$

der bis auf $\mathrm{PGL}_m(K)$-Isomorphie durch β eindeutig bestimmt ist. F ist also ein Funktionenkörper in $m-1$ Veränderlichen über k, dessen Skalarerweiterung mit K der rationale Funktionenkörper $K(T)$ ist.

Definition 3.14

Sei $\gamma \in \mathrm{H}^2(G, K^\times)$, dessen Schurindex $\mathrm{s}(\gamma)$ ein Teiler von $m \in \mathbb{N}$ sei. Der (bis auf $\mathrm{PGL}_m(K)$-Isomorphie) eindeutig bestimmte Teilkörper $F = \mathrm{F}_m(\gamma)$ von $K(T) = K(T_1, \ldots, T_{m-1})$ heißt der Brauerkörper der Dimension $m-1$ von γ.

Explizit ist $\mathrm{F}_m(\gamma)$ der Fixkörper von $K(T)$ unter $H = \{b_\sigma \sigma \mid \sigma \in G\}$.

Lemma 3.15

$\mathrm{F}_m(\gamma)$ ist eine reguläre Erweiterung von k.

Beweis:

Zwei Aussagen sind zu beweisen (siehe [Lan 93], Chap. VIII, §4):

(i) k ist algebraisch abgeschlossen in $\mathrm{F}_m(\gamma)$:
K ist algebraisch abgeschlossen in dem rationalen Funktionenkörper $K(T)$, so daß K der algebraische Abschluß von k in $K(T)$ ist. Daher ist $K \cap \mathrm{F}_m(\gamma) = k$ der algebraische Abschluß von k in $\mathrm{F}_m(\gamma)$.

(ii) $\mathrm{F}_m(\gamma)$ ist separabel erzeugt über k:
$K(T)$ ist separabel erzeugt über $k(T)$, weil K/k eine separable algebraische Erweiterung ist. Da $k(T)$ rationaler Funktionenkörper über k ist, ist $K(T)$ bereits über k separabel erzeugt. Als Teilkörper von $K(T)$ und endlich erzeugte Erweiterung von k ist damit $\mathrm{F}_m(\gamma)$ auch separabel erzeugt über k. □

Daß der Brauerkörper als virtueller Grundkörper, über dem sich das gegebene zentrale Einbettungsproblem mit korrespondierender 2-Kozykelklasse γ lösen läßt, überhaupt geeignet ist, liegt nun an der folgenden Aussage:

Satz 3.16

Sei K/k eine endliche Galoiserweiterung mit Galoisgruppe G. Sei $\gamma \in \mathrm{H}^2(G, K^\times)$, dessen Schurindex $\mathrm{s}(\gamma)$ ein Teiler von $m \in \mathbb{N}$ sei. Dann ist $\mathrm{F}_m(\gamma)$ ein Zerfällungskörper des verschränkten Produktes (K, G, γ).

Beweis:

Sei $F = \mathrm{F}_m(\gamma)$. Sei $\beta = (b_\sigma) \in \mathrm{H}^1(G, \mathrm{PGL}_m(K))$ ein Urbild von γ. Die – bisher mit H bezeichnete – Galoisgruppe

$$G_F = \mathrm{G}(FK/F) = \mathrm{G}(K(T)/F)$$

besteht also aus den Elementen

$$b_\sigma\sigma,\ \sigma \in G$$

und ist isomorph zu G.

Die Restriktionsabbildung $\mathrm{res}_{F/k} : \mathrm{Br}(k) \to \mathrm{Br}(F)$ aus (2.12) bildet die Untergruppe $\mathrm{Br}(K/k) \cong \mathrm{H}^2(G, K^\times)$ von $\mathrm{Br}(k)$ in die Untergruppe $\mathrm{Br}(FK/F) \cong \mathrm{H}^2(G_F, (FK)^\times)$ von $\mathrm{Br}(F)$ ab. Somit induziert $\mathrm{res}_{F/k}$ eine Abbildung (siehe (2.2) und [Lor 90], §30.2)

$$\mathrm{res}^G_{G_F} \ : \ \mathrm{H}^2(G, K^\times) \longrightarrow \mathrm{H}^2(G_F, (FK)^\times).$$

Die Behauptung, daß F Zerfällungskörper von (K, G, γ) ist, ist also gleichwertig damit, daß die Restriktion von γ zerfällt, d.h. $\mathrm{res}^G_{G_F}(\gamma) = 1$, was nun gezeigt wird.

Seien $a_\sigma \in \mathrm{GL}_m(K)$ die Urbilder der b_σ für $\sigma \in G$. Nach Abschnitt 2.1 und den bisherigen Ausführungen dieses Kapitels ist (siehe etwa (3.7))

$$c_{\sigma,\tau} = a_\sigma a_\tau^\sigma a_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G) \tag{3.19}$$

ein 2-Kozykel von G mit Werten in $K^\times$, der γ repräsentiert. Setzt man

$$u_\sigma := a_\sigma \sigma \qquad (\sigma \in G), \tag{3.20}$$

so liest sich (3.19) als

$$u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau} \qquad (\sigma, \tau \in G), \tag{3.21}$$

aufgefaßt in der Automorphismengruppe von $K(S)$ über k. Dabei ist der Automorphismus, der durch das Element $c_{\sigma,\tau} \in K^\times \trianglelefteq \mathrm{GL}_m(K)$ induziert wird, wie in (3.10) erklärt und multipliziert jedes homogene Element $\lambda(S) \in K(S)$ vom Grad 1 mit $c_{\sigma,\tau}$. Solch ein $\lambda(S)$ ist Quotient $g(S)/h(S)$ zweier homogener Polynome $g(S), h(S) \in K[S]$, $h(S) \neq 0$, wobei der Grad von g um 1 größer als der Grad von h ist. Ein vom Grad d homogenes Polynom $g(S) \in K[S]$ in m Veränderlichen ist von der Form

$$g(S) = g(S_1, \ldots, S_m) = \sum_{\nu:|\nu|=d} g_\nu S^\nu = \sum_{\substack{\nu=(\nu_1,\ldots,\nu_m):\\ |\nu|=d}} g_{(\nu_1,\ldots,\nu_m)} \prod_{j=1}^m S_j^{\nu_j};$$

der Betrag $|\nu|$ eines Multi-Indizes $\nu = (\nu_1, \ldots, \nu_m)$ ist durch $|\nu| := \nu_1 + \ldots + \nu_m$ definiert. Der Automorphismus $c_{\sigma,\tau}$ operiert auf $g(S)$ durch

$$\begin{aligned} g(S)^{c_{\sigma,\tau}} &= \sum_{\nu:|\nu|=d} g_\nu (c_{\sigma,\tau} S)^\nu \\ &= \sum_{\substack{\nu=(\nu_1,\ldots,\nu_m):\\ |\nu|=d}} g_{(\nu_1,\ldots,\nu_m)} \prod_{j=1}^m c_{\sigma,\tau}^{\nu_j} S_j^{\nu_j} \\ &= \sum_{\substack{\nu=(\nu_1,\ldots,\nu_m):\\ |\nu|=d}} \Big(\prod_{j=1}^m c_{\sigma,\tau}^{\nu_j}\Big)\, g_{(\nu_1,\ldots,\nu_m)} \prod_{j=1}^m S_j^{\nu_j} \\ &= c_{\sigma,\tau}^d g(S). \end{aligned}$$

Ist nun

$$\lambda = \lambda(S) = g(S)/h(S) = (\sum_{\nu:|\nu|=d} g_\nu S^\nu)/(\sum_{\nu:|\nu|=d-1} h_\nu S^\nu) \quad \text{(für ein } d > 0) \tag{3.22}$$

homogen vom Grad 1 in $K(S)$, so folgt

$$\lambda^{c_{\sigma,\tau}} = g(S)^{c_{\sigma,\tau}}/h(S)^{c_{\sigma,\tau}} = c_{\sigma,\tau}^{d-(d-1)}(g(S)/h(S)) = c_{\sigma,\tau}\lambda,$$

wie oben bereits behauptet wurde. Aus (3.21) ergibt sich damit

$$\lambda^{u_\sigma u_\tau} = c_{\sigma,\tau}\lambda^{u_{\sigma\tau}} \qquad (\sigma, \tau \in G).$$

Multipliziert man auf beiden Seiten mit λ^{-1}, so erhält man

$$\lambda^{u_\sigma - 1}\lambda^{u_\sigma(u_\tau - 1)} = c_{\sigma,\tau}\lambda^{u_{\sigma\tau}-1} \qquad (\sigma, \tau \in G). \tag{3.23}$$

Setzt man

$$\lambda_\sigma := \lambda^{u_\sigma - 1} \qquad (\sigma \in G), \tag{3.24}$$

so nimmt (3.23) die Form

$$\lambda_\sigma \lambda_\tau^{u_\sigma} = c_{\sigma,\tau}\lambda_{\sigma\tau} \qquad (\sigma, \tau \in G) \tag{3.25}$$

an. Da λ homogen vom Grad 1 ist, ist λ_σ homogen vom Grad 0 und liegt damit in $K(T)$. Der Automorphismus a_τ auf $K(S)$ induziert den Automorphismus b_τ auf $K(T)$, d.h. nach (3.20) ist

$$\lambda_\tau^{u_\sigma} = \lambda_\tau^{a_\sigma \sigma} = \lambda_\tau^{b_\sigma \sigma} \qquad (\sigma, \tau \in G), \tag{3.26}$$

wobei der rechte Ausdruck durch die Anwendung eines Elementes $b_\sigma\sigma \in G_F$ auf $\lambda_\tau \in K(T)$ erklärt ist. Also ist (3.25) gleichwertig mit

$$c_{\sigma,\tau} = \lambda_\sigma \lambda_\tau^{b_\sigma\sigma}\lambda_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G). \tag{3.27}$$

Da der F-Automorphismus $b_\sigma\sigma$ von $K(T)$ den k-Automorphismus $\sigma \in G$ von K induziert, zerfällt $c_{\sigma,\tau}$, betrachtet als 2-Kozykel von G_F mit Werten in $K(T)^\times$. Da der 2-Kozykel $c_{\sigma,\tau}$ ein Repräsentant von γ ist, folgt

$$\mathrm{res}_{G_F}^G(\gamma) = 1. \qquad \square$$

Sei k' eine beliebige Körpererweiterung von k. Sei $K' = Kk'$ mit Galoisgruppe $G' = \mathrm{G}(K'/k')$, die nach dem Translationssatz isomorph zu $\mathrm{G}(K/(K \cap k'))$ und damit isomorph zu einer Untergruppe von G ist. Dann gilt

$$\mathrm{F}_m(\gamma) \cdot k' = \mathrm{F}_m(\mathrm{res}^G_{G'}(\gamma)). \tag{3.28}$$

In die Sprache der Algebren läßt sich dies als

$$\mathrm{F}_m(\mathcal{A}_\gamma) \cdot k' = \mathrm{F}_m(\mathrm{res}_{k'/k}(\mathcal{A}_\gamma)) \tag{3.29}$$

übersetzen, wobei $\mathcal{A}_\gamma \in \mathrm{Br}(K/k)$ diejenige Klasse der zentral-einfachen k-Algebren bezeichne, die zu $\gamma \in \mathrm{H}^2(G, K^\times)$ gehört. (Siehe [Roq 63], §5, Eqns. (17), (18).)

Sei A_γ ein Repräsentant aus $\mathcal{A}_\gamma$.

Satz 3.17

Sei k'/k eine beliebige Körpererweiterung und k' ein Zerfällungskörper von A_γ. Dann ist $\mathrm{F}_m(\mathcal{A}_\gamma) \cdot k'$ ein rationaler Funktionenkörper in $m-1$ Veränderlichen über k'.

Beweis:

Gleichung (3.29) besagt, daß die Skalarerweiterung $\mathrm{F}_m(\mathcal{A}_\gamma) \cdot k'$ gerade der Brauerkörper $\mathrm{F}_m(\mathrm{res}_{k'/k}(\mathcal{A}_\gamma))$ über k' ist. Nach Voraussetzung ist $\mathrm{res}_{k'/k}(\mathcal{A}_\gamma) = 1$, d.h. die zentral-einfache k-Algebra $A_\gamma \otimes_k k'$ zerfällt über k'. Daher ist – siehe Gleichung (3.18) ff. mit k' anstelle von K – $\mathrm{F}_m(\mathrm{res}_{k'/k}(\mathcal{A}_\gamma))$ und damit auch $\mathrm{F}_m(\mathcal{A}_\gamma) \cdot k'$ ein rationaler Funktionenkörper in $m-1$ Veränderlichen über k'. □

Setzt man nun voraus, daß ein gegebenes zentrales Einbettungsproblem, welches zu γ gehöre, lösbar ist, so zerfällt nach Satz 2.7 die entsprechende zentral-einfache k-Algebra $A_\gamma = (K, G, \gamma)$ bereits über k. Nach vorstehendem Satz ist in diesem Fall also $\mathrm{F}_m(A_\gamma) \cdot k = F$ ein rationaler Funktionenkörper über k. Diese Tatsache ist wichtig im Hinblick auf die Anwendung des Hilbertschen Irreduzibilitätssatzes in Abschnitt 4.6.

Kapitel 4

Das allgemeine Verfahren

In diesem Kapitel werden die einzelnen Bausteine der Theorie erläutert. Zunächst wird der 2-Kozykel, der zu einem gegebenen Einbettungsproblem gehört, konkret als Produkt von Elementen aus $\mathrm{GL}_m(K)$ geschrieben, denn dies ist zur Berechnung des Brauerkörpers notwendig. Hernach wird ein virtueller Lösungskörper für das Einbettungsproblem angegeben, wobei dieser Körper noch Unbestimmte enthält. Ein wichtiges Hilfsmittel ist dabei das Lemma von Artin-Tate. Anschließend wird das definierende (oder Minimal-) Polynom des virtuellen Lösungskörpers über dem Brauerkörper berechnet, welches ebenfalls noch Unbestimmte enthält. Zum Abschluß wird der Hilbertsche Irreduzibilitätssatz auf dieses Polynom angewendet. Damit stellt man sicher, daß sich die Unbestimmten derart spezialisieren lassen (zumindest in der Theorie), daß man aus dem virtuellen auch einen expliziten Lösungskörper erhält.

4.1 Darstellung eines 2-Kozykels als Produkt von Matrizen

Sei K/k eine endliche Galoiserweiterung vom Grad n mit Galoisgruppe G.

Im Beweis des Satzes 3.16 wurde in (3.19) ein 2-Kozykel durch Elemente a_σ aus $\mathrm{GL}_m(K)$ definiert, deren Bilder $b_\sigma \in \mathrm{PGL}_m(K)$ als 1-Kozykelklasse das eindeutige Urbild der Klasse des 2-Kozykels unter der Abbildung (3.9) $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ definieren.

In dem am Ende von Abschnitt 2.4 erwähnten Beispiel aus [Som 96] wurde explizit ein 2-Kozykel $f : \mathrm{G} \times G \to \mu_2$ berechnet (siehe (2.18)), der zu dem dort vorgegebenen

zentralen Einbettungsproblem korrespondierte. Um Satz 3.16 auf dieses f anwenden zu können, müssen nun $a_\sigma \in \mathrm{GL}_m(K)$ berechnet werden, die die Gleichung (3.19) erfüllen. Dabei muß m nach Satz 3.6 ein Vielfaches des Schurindizes $\mathrm{s}(f)$ sein, damit die Klasse von f – aufgefaßt als 2-Kozykel $G \times G \to \mu_2 \hookrightarrow K^\times$ – im Bild von $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ liegt. Korollar 3.7 zeigte, daß

$$m = n \tag{4.1}$$

dies stets erfüllt.

Sei dazu V der k-Vektorraum K der Dimension n. Sei $e_\sigma,\ \sigma \in G$ eine k-Basis von V. Man definiert $a_\sigma \in \mathrm{Hom}_k(V, V)$ als den Automorphismus

$$a_\sigma(e_\tau) := f_{\sigma,\tau}\, e_{\sigma\tau} \qquad (\sigma, \tau \in G). \tag{4.2}$$

Die a_σ, aufgefaßt als Matrizen, liegen also in $\mathrm{GL}_m(K)$ mit $m = n$. Dann ist einerseits

$$(a_\sigma a_\tau^\sigma)(e_\rho) = f_{\sigma,\tau\rho} f_{\tau,\rho}^\sigma\, e_{\sigma\tau\rho} \qquad (\sigma, \tau, \rho \in G)$$

und andererseits

$$f_{\sigma,\tau} a_{\sigma\tau}(e_\rho) = f_{\sigma,\tau} f_{\sigma\tau,\rho}\, e_{\sigma\tau\rho} \qquad (\sigma, \tau, \rho \in G).$$

Da f ein 2-Kozykel ist, folgt

$$f_{\sigma,\tau} = a_\sigma a_\tau^\sigma a_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G). \tag{4.3}$$

4.2 Lemma von Artin-Tate

Vorgelegt seien zwei Gruppenerweiterungen

$$1 \longrightarrow A \xrightarrow{\ i\ } E \xrightarrow{\ \pi\ } G \longrightarrow 1 \tag{$*$}$$

und

$$1 \longrightarrow A' \xrightarrow{\ i'\ } E' \xrightarrow{\ \pi'\ } G' \longrightarrow 1 \tag{$**$}$$

von G bzw. G' mit abelschem Kern A bzw. A' sowie Homomorphismen $t : A' \to A$ und $\theta : G' \to G$. Zu $(*)$ gehöre der 2-Kozykel f und zu $(**)$ f'. In dem folgenden Satz wird ein Kriterium für die Existenz eines Homomorphismus $\Theta : E' \to E$ angegeben, der das Diagramm

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \qquad (*) \\
 & & {\scriptstyle t}\uparrow & & {\scriptstyle \Theta}\uparrow & & {\scriptstyle \theta}\uparrow & & \\
1 & \longrightarrow & A' & \longrightarrow & E' & \longrightarrow & G' & \longrightarrow & 1 \qquad (**)
\end{array}
\tag{4.4}
$$

kommutativ ergänzt. G' operiert auf A via θ. $t^* : \mathrm{H}^2(G', A') \to \mathrm{H}^2(G', A)$ sei der durch t und $\theta^* : \mathrm{H}^2(G, A) \to \mathrm{H}^2(G', A)$ der durch θ induzierte Homomorphismus von Kohomologiegruppen.

Lemma 4.1 (Artin-Tate)

Unter obigen Voraussetzungen sind die beiden folgenden Behauptungen äquivalent:

(a) Es existiert ein Homomorphismus $\Theta : E' \to E$, der das Diagramm (4.4) kommutativ ergänzt.

(b) t ist ein G-Homomorphismus mit $t^*((f')) = \theta^*((f))$.

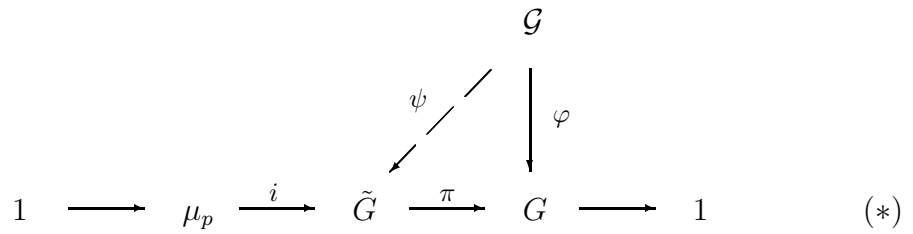
Beweis:

Siehe [A-T 61], Chap. 13, p. 174 - 180, Thm. 2. □

4.3 Konstruktion eines virtuellen Lösungskörpers

Sei nun k ein Körper, der die p-ten Einheitswurzeln μ_p für eine Primzahl p enthalte und von der Charakteristik $\operatorname{char} k \neq p$ sei. $\mathcal{G}$ bezeichne die absolute Galoisgruppe von k. Es sei K/k eine endliche Galoiserweiterung mit $G = \mathrm{G}(K/k)$, für die ein zentrales Einbettungsproblem

(4.5)



für eine endliche Gruppe $\tilde{G}$ vorgelegt sei. Es gehe $f \in \mathrm{Z}^2(G, \mu_p)$ mit $(*)$ einher. Zur genaueren Unterscheidung bezeichne (f) die Klasse in $\mathrm{H}^2(G, \mu_p)$ und $[f]$ die Klasse in $\mathrm{H}^2(G, K^\times)$, wobei $[f]$ gelegentlich auch für die Klasse $[A_f] \in \mathrm{Br}(K/k)$ der zu f gehörenden zentral-einfachen k-Algebra $A_f = (K, G, f)$ steht.

Sei $m \in \mathbb{N}$ derart, daß der Brauerkörper $F = \mathrm{F}_m([f])$ zu $[f]$ existiert (z.B. enthalte m den Primfaktor p). Man setze

$$k_F = Fk = F, \qquad K_F = FK \qquad \text{und} \qquad G_F = \mathrm{G}(K_F/k_F) \cong G.$$

Nach Satz 3.16 ist F ein Zerfällungskörper von f. Wegen (3.27) gibt es somit $\lambda_\sigma \in K_F^\times$ mit

$$f_{\sigma,\tau} = \lambda_\sigma \lambda_\tau^\sigma \lambda_{\sigma\tau}^{-1} \qquad (\sigma, \tau \in G_F), \tag{4.6}$$

wobei $\lambda_\tau^\sigma, \sigma \in G_F$ abkürzend für die in (3.26) erklärte Operation $\lambda_\tau^{b_\sigma \sigma}, \sigma \in G$ steht.

Wegen $f_{\sigma,\tau}^p = 1$ folgt aus (4.6)

$$\lambda_{\sigma\tau}^p = \lambda_\sigma^p \, (\lambda_\tau^p)^\sigma \qquad (\sigma, \tau \in G_F). \tag{4.7}$$

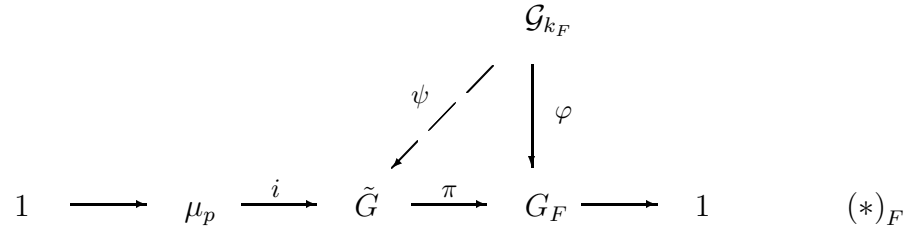
λ_σ^p ist also ein 1-Kozykel von G_F mit Werten in $K_F^\times$. Nach Hilbert 90 gibt es ein $c_F \in K_F^\times$ mit

$$\lambda_\sigma^p = \frac{c_F^\sigma}{c_F} \qquad (\sigma \in G_F), \tag{4.8}$$

dessen Konstruktion im Beweis zu Satz 2.2 erläutert wurde.

Aus (4.6) folgt mit dem Satz 2.5 von Hoechsmann, daß das zentrale Einbettungsproblem

(4.9)



lösbar ist, wobei $\mathcal{G}_{k_F}$ die absolute Galoisgruppe von k_F bezeichne. Den zu $(*)_F$ gehörigen 2-Kozykel identifiziert man wegen $G_F \cong G$ mit f. In dem Diagramm (4.4) wird nun $(*)$ durch $(*)_F$ ersetzt.

Es sei

$$L_F = K_F(\gamma_F) \qquad \text{mit} \qquad \gamma_F := \sqrt[p]{c_F}.$$

L_F/K_F ist eine Kummererweiterung mit zyklischer Galoisgruppe

$$\mathrm{G}(L_F/K_F) = <\varrho> \cong \mu_p,$$

die durch einen K_F-Automorphismus $\varrho : L_F \to L_F$ erzeugt werde. Für $(**)$ wird die Sequenz

$$1 \longrightarrow \mathrm{G}(L_F/K_F) \longrightarrow \mathrm{G}(L_F/k_F) \longrightarrow G_F \longrightarrow 1 \qquad (**)_F$$

eingesetzt, die aus dem Hauptsatz der Galoistheorie abgeleitet wird.

Für einen Automorphismus $\sigma \in G_F$ bezeichne

$$\tilde{\sigma} \in \mathrm{G}(L_F/k_F)$$

eine Fortsetzung von σ auf L_F. Wegen

$$\tilde{\sigma}(\gamma_F)^p = \tilde{\sigma}(\gamma_F^p) = \tilde{\sigma}(c_F) = \sigma(c_F)$$

und (4.8) folgt

$$\tilde{\sigma}(\gamma_F) = \sqrt[p]{\sigma(c_F)} = \sqrt[p]{\lambda_\sigma^p\, c_F} = \lambda_\sigma\, \gamma_F \qquad (\sigma \in G_F). \tag{4.10}$$

Die injektive Abbildung

$$t \ : \quad \mathrm{G}(L_F/K_F) \longrightarrow \mu_p \ : \quad \varrho \longmapsto t(\varrho) := \frac{\varrho(\gamma_F)}{\gamma_F}$$

ist ein Homomorphismus, denn für beliebige $\varrho', \varrho'' \in \mathrm{G}(L_F/K_F)$ gilt

$$(\varrho'\varrho'')(\gamma_F) = \varrho'(\varrho''(\gamma_F)) = \varrho'(t(\varrho'')\gamma_F) = t(\varrho'')\,\varrho'(\gamma_F) = t(\varrho')\,t(\varrho'')\,\gamma_F.$$

Da t nicht-trivial und p eine Primzahl ist, ist t sogar ein Isomorphismus. Das Diagramm (4.4) wird somit zu

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_p & \longrightarrow & \tilde{G} & \longrightarrow & G_F & \longrightarrow & 1 \qquad (*)_F \\ & & {\scriptstyle t}\uparrow\cong & & {\scriptstyle\Theta}\,\vdots\uparrow\cong & & \| & & \\ 1 & \longrightarrow & \mathrm{G}(L_F/K_F) & \longrightarrow & \mathrm{G}(L_F/k_F) & \longrightarrow & G_F & \longrightarrow & 1 \qquad (**)_F. \end{array} \tag{4.11}$$

Existiert nämlich ein solcher Homomorphismus Θ, der (4.11) kommutativ ergänzt, so ist er bereits ein Isomorphismus, da t bijektiv ist.

Satz 4.2

L_F ist ein virtueller Lösungskörper für das in (4.9) definierte Einbettungsproblem.

Beweis:

Die Behauptung ist gleichwertig zur Existenz eines Isomorphismus $\Theta : \mathrm{G}(L_F/k_F) \to \tilde{G}$. Zum Beweis der Existenz von Θ wird das Lemma von Artin-Tate herangezogen.

Zunächst ist nachzuweisen, daß t ein G_F-Homomorphismus ist. Dies reduziert sich auf den Beweis der Identität

$$t(\varrho^\sigma) = t(\varrho)^\sigma \qquad (\sigma \in G_F), \tag{4.12}$$

in μ_p. G_F operiert auf $\mathrm{G}(L_F/K_F)$ via $\varrho^\sigma = \tilde{\sigma}\varrho\tilde{\sigma}^{-1}$. Auf μ_p operiert G_F durch Anwendung des Automorphismus auf eine p-te Einheitswurzel; wegen $\mu_p \subseteq k \subseteq k_F$ ist die Operation hier trivial. (4.12) ist also gleichwertig zu (man multipliziere noch mit γ_F):

$$(\tilde{\sigma}\varrho\tilde{\sigma}^{-1})(\gamma_F) = \varrho(\gamma_F) \qquad (\sigma \in G_F). \tag{4.13}$$

Sei $\sigma \in G_F$ beliebig. Dann ist nach (4.10)

$$(\varrho\tilde{\sigma})(\gamma_F) \ = \ \varrho(\tilde{\sigma}(\gamma_F)) \ = \ \varrho(\lambda_\sigma\gamma_F) \ = \ \lambda_\sigma\,\varrho(\gamma_F),$$

da $\lambda_\sigma \in K_F^\times$ unter ϱ fix bleibt. Andererseits folgt mit der Definition von t

$$\begin{aligned}(\tilde{\sigma}\varrho)(\gamma_F) &= \tilde{\sigma}(\varrho(\gamma_F)) = \tilde{\sigma}(t(\varrho)\gamma_F) = t(\varrho)\,\tilde{\sigma}(\gamma_F) = t(\varrho)\,\lambda_\sigma\gamma_F \\ &= \lambda_\sigma\,\varrho(\gamma_F),\end{aligned}$$

was (4.13) zeigt.

Nun bleibt noch die Gültigkeit von $t^*((f')) = \theta^*((f))$, d.h.

$$t(f'_{\sigma,\tau}) = f_{\sigma,\tau} \qquad (\sigma,\tau \in G_F) \tag{4.14}$$

zu zeigen, wobei $f' \in \mathrm{Z}^2(G_F, \mathrm{G}(L_F/K_F))$ der zu $(**)_F$ korrespondierende 2-Kozykel ist. Seien $\sigma, \tau \in G_F$ beliebig. Sei

$$\varrho' := f'_{\sigma,\tau} = \tilde{\sigma}\,\tilde{\tau}\,\widetilde{\sigma\tau}^{-1} \in \mathrm{G}(L_F/K_F).$$

Dann ist wieder mit (4.10)

$$\begin{aligned}(\tilde{\sigma}\tilde{\tau})(\gamma_F) &= \tilde{\sigma}(\tilde{\tau}(\gamma_F)) = \tilde{\sigma}(\lambda_\tau\gamma_F) = \lambda_\tau^\sigma\,\tilde{\sigma}(\gamma_F) \\ &= \lambda_\tau^\sigma\,\lambda_\sigma\,\gamma_F = \lambda_\sigma\,\lambda_\tau^\sigma\,\gamma_F\end{aligned}$$

und andererseits

$$\begin{aligned}(\varrho'\,\widetilde{\sigma\tau})(\gamma_F) &= \varrho'(\widetilde{\sigma\tau}(\gamma_F)) = \varrho'(\lambda_{\sigma\tau}\gamma_F) = \lambda_{\sigma\tau}\,\varrho'(\gamma_F) \\ &= \lambda_{\sigma\tau}\,t(\varrho')\,\gamma_F = t(\varrho')\,\lambda_{\sigma\tau}\,\gamma_F\end{aligned}$$

Damit ergibt sich (4.14):

$$t(f'_{\sigma,\tau}) = t(\varrho') = \lambda_\sigma\,\lambda_\tau^\sigma\,\lambda_{\sigma\tau}^{-1} = f_{\sigma,\tau} \qquad (\sigma,\tau \in G_F).$$

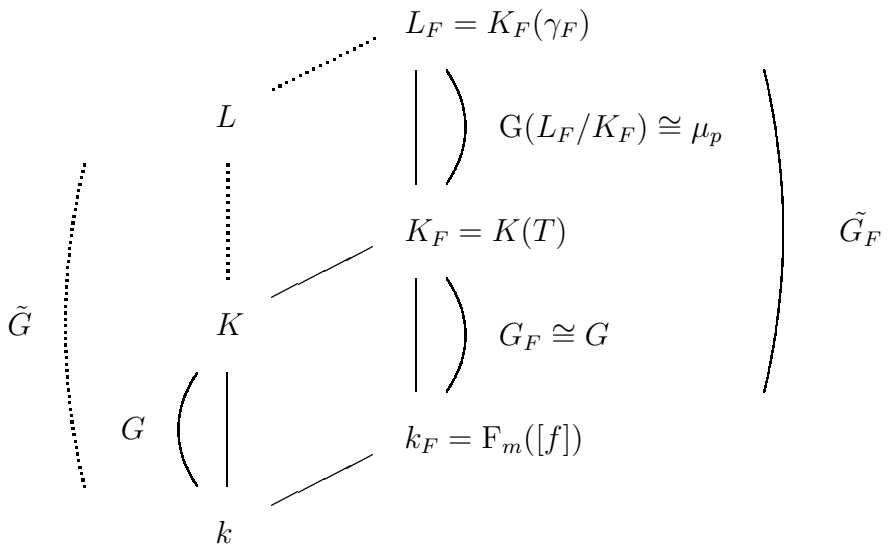
□

An dieser Stelle ist eine historische Anmerkung angebracht. Der vorstehende Satz 4.2 ist eine Variante eines allgemeinen Ergebnisses von Witt. In [Wit 36], Kap. VI wird nämlich ein Verfahren zur Konstruktion eines Körpers beschrieben, dessen Galoisgruppe über dem Grundkörper (von beliebiger Charakteristik) die Quaternionengruppe ist. Dies geschieht dort allerdings auf völlig andere Art und Weise und ist wesentlich schwieriger nachzuvollziehen als obiger Beweis von Satz 4.2.

4.4 Das definierende Polynom von L_F/k_F

Die folgende Abbildung veranschaulicht die Erkenntnisse des vorhergehenden Abschnittes.

(4.15)



Sei k ein algebraischer Zahlkörper. Durch Spezialisierung von $T = (T_1, \ldots, T_{m-1})$ in $\gamma_F(T) = \sqrt[p]{c_F(T)}$ gilt es also, aus L_F einen expliziten Lösungskörper L für das zentrale Einbettungsproblem (4.5) – vorausgesetzt, es ist lösbar – zu gewinnen. Dies geschieht, indem man ein definierendes Polynom von L_F/k_F berechnet, um anschließend mit Hilfe des Hilbertschen Irreduzibilitätssatzes ein definierendes Polynom für L/k zu erhalten, dessen Galoisgruppe $\tilde{G}$ isomorph zu $\tilde{G}_F$ ist.

γ_F ist ein primitives Element von L_F/K_F. Sei $\vartheta_F = \vartheta_F(T)$ ein solches für K_F/k_F, also $K_F = k_F(\vartheta_F)$. Die Existenz von ϑ_F folgt aus der Tatsache, daß die in Frage stehende Erweiterung endlich und separabel ist ('Satz vom primitiven Element'). Es seien $p_F(T, X) \in k_F[X]$ und $q_F(T, X) \in K_F[X]$ die definierenden Polynome von ϑ_F über k_F bzw. von γ_F über K_F. Bezeichnet N_{K_F/k_F} die auf den Polynomring $K_F[X]$ fortgesetzte Normabbildung von K_F/k_F, so ist

$$r_F(T, X) = \mathrm{N}_{K_F/k_F}(q_F(T, X)) \in k_F[X] \tag{4.16}$$

das gesuchte definierende Polynom von L_F/k_F mit Nullstelle γ_F. Dabei muß $q_F(T, X)$ gegebenenfalls durch $q_F(T, X - l\vartheta_F)$ für ein geeignetes $l \in \mathbb{Z}$ ersetzten werden, sollte sich r_F zunächst als Vielfaches eines irreduziblen Polynoms erweisen.

Explizit erhält man r_F wie folgt: Man schreibe q_F in der Form

$$q_F(T,X) = \sum_{i=0}^{n} a_i(T)X^i \qquad \text{(für gewisse } a_i(T) \in K_F\text{)}$$

sowie die Koeffizienten $a_i(T)$ in der Form

$$a_i(T) = g_i(T, \vartheta_F) \qquad \text{(für gewisse } g_i(T,X) \in k_F[X]\text{)}$$

und setze

$$\tilde{q_F}(T,X,Y) := \sum_{i=0}^{n} g_i(T,Y)X^i.$$

Dann liefert die Resultante bezüglich der Variablen Y

$$r_F(T,X) = \mathrm{Res}(p_F(T,Y), \tilde{q_F}(T, X - lY, Y), Y) \tag{4.17}$$

das Gewünschte. (Siehe [Coh 93], Ch. 3.6.2, Algor. 3.6.4.)

4.5 Brauerkörper und Brauer-Severi Varietäten

Es sei k ein Körper. $\mathbb{P}_k^{m-1}$ bezeichne den $(m-1)$-dimensionalen projektiven Raum, aufgefaßt als k-Schema. In diesem Abschnitt wird unter einer *k-Varietät* ein algebraisches k-Schema verstanden, das geometrisch reduziert und geometrisch irreduzibel ist. Sei V eine $(m-1)$-dimensionale projektive k-Varietät. V ist eine *Brauer-Severi Varietät*, wenn es eine algebraische separable Erweiterung K/k gibt, so daß V über K isomorph zum projektiven Raum über K ist, d.h.

$$V \otimes_k K \cong \mathbb{P}_K^{m-1} = \mathbb{P}_k^{m-1} \otimes_k K.$$

Neben dieser Definition durch 'Galois-Abstieg' (engl. *'Galois descent'*) gibt es noch den direkten Weg, indem man eine Brauer-Severi Varietät als Teil-Varietät einer Grassmann Varietät erklärt. (Siehe [Ser 95], Chap. X, §6; [Ker 90], Kap. V, §30; [ArM 82], §1.)

In [Roq 63], §1 wird erwähnt, daß Brauerkörper gerade die Funktionenkörper von Brauer-Severi Varietäten sind, ohne daß dazu allerdings ein Beweis angegeben wird. Genauer wird dies in [Kan 90], §2 behandelt, indem dort der homogene Koordinatenring der Brauer-Severi Varietät konstruiert wird:

Es sei $[f] \in \mathrm{H}^2(G, K^\times)$ eine 2-Kozykelklasse vom Exponenten $e = \exp(f)$. Der Schurindex $\mathrm{s}(f)$ teile m, so daß der zugehörige Brauerkörper $\mathrm{F}_m([f])$ existiert. Die Monome vom Grad e in $K[X] = K[X_1, \ldots, X_m]$ erzeugen eine graduierte Teil-Algebra $K_e[X]$ über K. Für ein vom Grad er, $r \in \mathbb{N}_0$ homogenes Polynom $g(X) \in K_e[X]$ definiert man eine G-Operation durch

$$g(X)^\sigma := \lambda_\sigma^{-r}\, g(X)^{u_\sigma} \qquad (\sigma \in G), \tag{4.18}$$

wobei $u_\sigma = a_\sigma\sigma$ wie in (3.20) für gewisse $a_\sigma \in \mathrm{GL}_m(K)$ definiert ist und λ_σ ein 1-Kozykel von G mit Werten in $K^\times$ ist, der

$$\lambda_\sigma\, \lambda_\tau^\sigma\, \lambda_{\sigma\tau}^{-1} = f_{\sigma,\tau}^e = 1 \qquad (\sigma, \tau \in G)$$

erfüllt. Die Argumentation ist ähnlich der in (4.7) mit dem Unterschied, daß hier die Werte von λ_σ als in $K^\times$ liegend angenommen werden. Es sei

$$R := K_e[X]^G \tag{4.19}$$

die graduierte k-Algebra der G-Invarianten von $K_e[X]$ unter der Operation (4.18), die bis auf Isomorphie unabhängig von der Wahl von λ_σ ist. In dieser Sprechweise ist der entsprechende Brauerkörper zu f

$$\begin{aligned} \mathrm{F}_m([f]) &= \{\frac{g(X)}{h(X)} \mid g, h \in R \text{ homogen mit } \mathrm{grad}(g) = \mathrm{grad}(h)\} \\ &= \{g(T) \in K(T)^H\} \end{aligned} \tag{4.20}$$

mit

$$H = \{b_\sigma\sigma \mid b_\sigma \in \mathrm{PGL}_m(K) \text{ ist Bild von } a_\sigma \in \mathrm{GL}_m(K) \text{ für } \sigma \in G\},$$

denn $K(T)$ ist der Teilkörper aller vom Grad 0 homogenen Elemente von $K(X)$ (siehe Abschnitt 3.4).

Die durch den homogenen Koordinatenring R definierte projektive k-Varietät

$$\mathrm{V}_m([f]) := \mathrm{Proj}(R) \tag{4.21}$$

ist eine Brauer-Severi Varietät der Dimension $m-1$ über k (siehe [Kan 90], §2, Thm. 1). Wegen (4.20) ist klar, daß $F = \mathrm{F}_m([f])$ der Funktionenkörper von $V = \mathrm{V}_m([f])$ ist, d.h.

$$F = k(V).$$

Feststellung 4.3

Zwischen den folgenden Mengen lassen sich also Bijektionen herstellen:

(a) Die Menge der Isomorphieklassen von Brauer-Severi Varietäten V der Dimension $m-1$ über k, die von K zerfällt werden (i.e. $V \otimes_k K \cong \mathbb{P}_K^{m-1}$).

(b) Die Menge der Isomorphieklassen von Brauerkörpern F.

(c) Die Menge der 1-Kozykelklassen $(b_\sigma) \in \mathrm{H}^1(G, \mathrm{PGL}_m(K))$.

(d) Die Menge der 2-Kozykelklassen $[f] \in \mathrm{H}^2(G, K^\times)$, die im Bild der injektiven Abbildung $\mathrm{H}^1(G, \mathrm{PGL}_m(K)) \to \mathrm{H}^2(G, K^\times)$ liegen (i.e. $\mathrm{s}(f) \mid m$).

(e) Die Menge der Äquivalenzklassen zentral-einfacher k-Algebren A vom Grad m (i.e. $\dim_k A = m^2$), die von K zerfällt werden.

Beweis:

Oben wurde der Zusammenhang zwischen den Mengen aus (a) und (e) dargestellt. Kapitel 3 beschrieb ausführlich, wie die Mengen aus (b), (c) und (d) korrespondieren. Die Bijektion schließlich zwischen den Mengen aus (d) und (e) wird durch den Isomorphismus $\mathrm{H}^2(G, K^\times) \cong \mathrm{Br}(K/k)$ (Satz 2.6) induziert. □

Beispiel 4.4

Die Brauer-Severi Varietät der Quaternionenalgebra (a, b) wird in der projektiven Form durch

$$X^2 - aY^2 - bZ^2 = 0$$

repräsentiert. Affin bedeutet das die Gleichung (2.16)

$$X^2 - aY^2 = b.$$

Beweis:

Siehe [ArM 82], Rem. 1.6.2., p. 196. □

Abschließend wird nun beschrieben, wie der Funktionenkörper einer Kurve vom Grad 2 über dem Grundkörper k und der rationale Funktionenkörper $k(T)$ in einer Unbestimmten T zusammenhängen.

Es sei C eine Kurve vom Grad 2, gegeben durch

$$C: \quad f(X,Y) = 0 \qquad \text{mit} \qquad f(X,Y) \in k[X,Y]. \tag{4.22}$$

Für einen beliebigen k-rationalen Punkt (x,y) aus $C(k)$, d.h. $x, y \in k$ mit $f(x,y) = 0$, sei

$$T := \frac{Y-y}{X-x}. \tag{4.23}$$

Behauptet wird: X und Y sind rationale Funktionen von T über k. Aus (4.23) folgt nämlich

$$Y = y + T(X-x), \tag{4.24}$$

so daß man aus $f(X, y+T(X-x)) = 0$ eine quadratische Gleichung für X der Form

$$\alpha_2(T)\, X^2 + \alpha_1(T)\, X + \alpha_0(T) = 0 \tag{4.25}$$

für gewisse $\alpha_i(T) \in k(T),\ i = 0,1,2$ erhält. Eine Lösung von (4.24) lautet $X = x$ wegen $f(x,y) = 0$. Da die Summe der beiden Nullstellen von (4.25) gleich $-\frac{\alpha_1(T)}{\alpha_2(T)}$ ist, läßt sich die andere Nullstelle aus x und $-\frac{\alpha_1(T)}{\alpha_2(T)}$ berechnen. Somit lassen sich X und Y aufgrund von (4.24) als rationale Funktionen

$$X = g(T) \in k(T) \qquad \text{und} \qquad Y = h(T) \in k(T) \tag{4.26}$$

von T über k schreiben, so daß obige Behauptung bewiesen ist.

Natürlich gilt wegen (4.22)

$$f(g(T), h(T)) = 0.$$

Somit erhält man einen k-Isomorphismus

$$k(C) \xrightarrow{\cong} k(T): \qquad X \longmapsto g(T), \quad Y \longmapsto h(T) \tag{4.27}$$

von Körpern.

4.6 Der Hilbertsche Irreduzibilitätssatz

In diesem und dem nächsten Abschnitt wird gezeigt, daß man das die Erweiterung L_F/k_F definierende Polynom $r_F(T, X)$ auf unendlich viele Weisen derart spezialisieren kann, daß man ein definierendes Polynom für L/k erhält, sofern k eine gewisse Eigenschaft besitzt. Am Ende des anschließenden Abschnittes erhält man damit einen expliziten Lösungskörper, womit der theoretische Teil dieser Arbeit abgeschlossen ist.

Ist $k = \mathbb{Q}$, so stammt das entscheidende Resultat von Hilbert selbst:

Satz 4.5 (Hilbertscher Irreduzibilitätssatz)

Sei $g(T_1, \ldots, T_{m-1}, X) \in \mathbb{Q}(T_1, \ldots, T_{m-1})[X]$ ein irreduzibles Polynom mit Galoisgruppe $\tilde{G} = \mathrm{G}(g(T_1, \ldots, T_{m-1}, X))$. Dann existieren unendlich viele Mengen von rationalen Zahlen $t_1, \ldots, t_{m-1}$ derart, daß $g(t_1, \ldots, t_{m-1}, X) \in \mathbb{Q}[X]$ irreduzibel ist und die Galoisgruppe $\mathrm{G}(g(t_1, \ldots, t_{m-1}, X)) \cong \tilde{G}$ ist.

Beweis:

Siehe [Hil 92], Thm. III und IV; [Had 78], Chap. 4.2, Thm. 36. □

Allgemeiner definiert man einen Körper k als *hilbertsch*, wenn der Hilbertsche Irreduzibilitätssatz für k anstelle von $\mathbb{Q}$ richtig bleibt, wobei die Koeffizienten von $g(t_1, \ldots, t_{m-1}, X)$ definiert sein müssen. Beispiele hilbertscher Körper sind die algebraischen Zahlkörper – insbesondere also auch $\mathbb{Q}$, siehe oben – und die unendlichen, endlich erzeugten Körper. Die lokalen Körper $\mathbb{Q}_p$, p Primzahl oder $p = \infty$, sind dagegen nicht hilbertsch.

(Siehe auch [Mat 88], Ab. (1.5); [Ser 92], Chap. 3, Prop. 3.3.5; [Lan 93], Chap. 9.)

4.7 Konstruktion eines expliziten Lösungskörpers

Sei k ein algebraischer Zahlkörper mit $\mu_p \subseteq k$. Sei K eine endliche Galoiserweiterung von k mit $G = \mathrm{G}(K/k)$. Setzt man voraus, daß ein gegebenes zentrales Einbettungsproblem $\mathcal{E}$ mit korrespondierendem 2-Kozykel f lösbar ist, so zerfällt nach Satz 2.7 die zugehörige zentral-einfache k-Algebra $A_f = (K, G, f)$ bereits über k. Nach Satz 3.17 ist das Kompositum $k_F = Fk = F$ des Brauerkörpers $F = \mathrm{F}_m([A_f])$ mit k ein rationaler Funktionenkörper in $m - 1$ Unbestimmten über k:

(4.28) $$k_F = F = k(T') = k(T'_1, \ldots, T'_{m-1}).$$

Allerdings ist i.a. die in Abschnitt 3.4 gewählte Unbestimmte T kein Element aus F, wie anhand der Beispiele im folgenden Kapitel klar werden wird. Um dies deutlich zu machen, wurde hier eine Unbestimmte T' gewählt, die von T abhängt. Denn wie gewohnt ist

(4.29) $$K_F = FK = K(T) = K(T_1, \ldots, T_{m-1})$$

rationaler Funktionenkörper in $m-1$ Veränderlichen mit $G_F = \mathrm{G}(K_F/k_F) \cong G$.

Es sei $r_F(T, X) \in F[X]$ das definierende irreduzible Polynom von $L_F = K_F(\gamma_F(T)) = K(\gamma_F(T))(T)$ über F mit Galoisgruppe $\tilde{G_F}$. r_F wird gemäß Abschnitt 4.4 (siehe Gleichung (4.16)) berechnet. Der (verallgemeinerte) Hilbertsche Irreduzibilitätssatz sichert nun die Existenz unendlich vieler Spezialisierungen $T \mapsto t \in k$ – damit wird dann auch zugleich das von T abhängige T' spezialisiert –, so daß $r(X) = r_F(t, X)$ irreduzibel über k bleibt. Die dadurch beschriebene Erweiterung L/k hat eine zu $\tilde{G_F}$ isomorphe Galoisgruppe $\tilde{G}$. Damit ist gezeigt:

Satz 4.6

Sei k ein algebraischer Zahlkörper, der die p-ten Einheitswurzeln μ_p für eine Primzahl p enthalte. Sei L_F ein virtueller Lösungskörper eines gegebenen zentralen Einbettungsproblems der Form (4.5). Ist das Einbettungsproblem über k lösbar, so lassen sich die Unbestimmten $T_1, \ldots, T_{m-1}$ auf unendlich viele Weisen derart spezialisieren, daß der damit aus L_F hervorgehende Körper L ein expliziter Lösungskörper von (4.5) mit $\mathrm{G}(L/k) \cong \tilde{G}$ ist. □

Ist konkret $k = \mathbb{Q}$ und $K = \mathbb{Q}(\vartheta)$, so ist

(4.30) $$F = \mathbb{Q}(T'), \qquad K_F = \mathbb{Q}(\vartheta)(T) \qquad \text{und} \qquad L_F = \mathbb{Q}(\vartheta, \gamma_F(T))(T).$$

Obiger Satz 4.5 besagt also, daß man auf unendlich viele Weisen T durch $t = (t_1, \ldots, t_{m-1})$, $t_i \in \mathbb{Q}$ ersetzen kann, so daß das Polynom $r(X)$ irreduzibel über $\mathbb{Q}$ ist und seine Galoisgruppe isomorph zu der von $r_F(T, X)$ ist. Dadurch gewinnt man zugleich ein primitives Element

(4.31) $$\gamma = \gamma_F(t)$$

der Erweiterung L/K und somit nach Satz 4.6 einen expliziten Lösungskörper $L = \mathbb{Q}(\vartheta, \gamma)$ des gegebenen Einbettungsproblems über $\mathbb{Q}$.

Die Frage, wie man effektiv beim Hilbertschen Irreduzibilitätssatz zu expliziten Spezialisierungen gelangt, wird von EKEDAHL in [Eke 90] behandelt, soll hier aber nicht weiter betrachtet werden.

Kapitel 5

Beispiele

In diesem abschließenden Kapitel soll anhand zweier Beispiele die Theorie praktisch umgesetzt werden. Eines beschäftigt sich mit einem Gegenbeispiel zum Hasseschen Normensatz, das andere mit dem in der Einleitung erläuterten Satz von Serre, der diese Arbeit motivierte.

5.1 Berechnung der Matrizen

Sei $k = \mathbb{Q}$. Sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ mit $a, b \in \mathbb{Q}^\times$ derart, daß

$$G = \mathrm{G}(K/k) \cong V_4$$

ist. Der Grad der Erweiterung ist also $n = (K : k) = 4$. G werde dabei durch die $\mathbb{Q}$-Automorphismen σ und τ aufgespannt, die durch

$$\sigma(\sqrt{a}) = -\sqrt{a}, \quad \sigma(\sqrt{b}) = \sqrt{b}, \quad \tau(\sqrt{a}) = \sqrt{a}, \quad \tau(\sqrt{b}) = -\sqrt{b}$$

definiert sind. Der 2-Kozykel f, der zu der Gruppenerweiterung

$$1 \longrightarrow \mu_2 \longrightarrow D_4 \longrightarrow V_4 \longrightarrow 1 \qquad (*)$$

gehört, lautet nach (2.18):

(5.1)

$f_{\rho,\eta}$	id	σ	τ	$\sigma\tau$
id	1	1	1	1
σ	1	1	-1	-1
τ	1	1	1	1
$\sigma\tau$	1	1	-1	-1

Wegen $\mu_2 \subseteq K$ kann man f als 2-Kozykel von G mit Werten in $K^\times$ auffassen. Die zugehörige zentral-einfache k-Algebra (K, G, f) hat offensichtlich den Exponenten $\exp((K, G, f)) = 2 = \exp(f)$. Im Zahlkörperfall ist der Schurindex gleich dem Exponenten (siehe [Lor 90], §30.3, Bem. 1), d.h. $\mathrm{s}(f) = \exp(f) = 2$.

Zunächst wird gemäß Abschnitt 4.1 vorgegangen, d.h. man wähle $m = n = 4$ wie in (4.1); m ist also in der nun folgenden Konstruktion nicht minimal (siehe Bemerkung nach Korollar 3.7 in Abschnitt 3.2). Nach (4.2) erhält man

$a_\rho(e_\eta)$	e_{id}	e_σ	e_τ	$e_{\sigma\tau}$
a_{id}	e_{id}	e_σ	e_τ	$e_{\sigma\tau}$
a_σ	e_σ	e_{id}	$-e_{\sigma\tau}$	$-e_\tau$
a_τ	e_τ	$e_{\sigma\tau}$	e_{id}	e_σ
$a_{\sigma\tau}$	$e_{\sigma\tau}$	e_τ	$-e_\sigma$	$-e_{\mathrm{id}}$.

Nimmt man nun die Standard-Basis

$$e_{\mathrm{id}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad e_\sigma = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_\tau = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_{\sigma\tau} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

so haben die Matrizen folgendes Aussehen:

$$
\begin{aligned}
a_{\mathrm{id}} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, & a_{\sigma} &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \\
a_{\tau} &= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, & a_{\sigma\tau} &= \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.
\end{aligned} \tag{5.2}
$$

Sie erfüllen somit (4.3)

$$
f_{\rho,\eta} = a_\rho a_\eta^\rho a_{\rho\eta}^{-1} = a_\rho a_\eta a_{\rho\eta}^{-1} \qquad (\rho, \eta \in G), \tag{5.3}
$$

letzteres wegen der trivialen Operation von G auf μ_2.

In dem hier vorliegenden speziellen Fall kann man aber die Matrizen a_ρ nach einem Verfahren, welches in [Som 96], Beweis zu Satz 8.5, S. 86 ff. beschrieben ist und aus [Sna 89], Chap. 3.42, Thm. 3.50 stammt, bereits in $\mathrm{GL}_2(K)$ konstruieren; dann ist hier also

$$m = 2$$

also in der Tat minimal gewählt. Für

$$
\begin{aligned}
a_{\mathrm{id}} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & a_{\sigma} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\
a_{\tau} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & a_{\sigma\tau} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.
\end{aligned} \tag{5.4}
$$

gilt nämlich ebenfalls die Identität (5.3). Die Elemente

$$b_\rho = a_\rho \mod K^\times \qquad (\rho \in G)$$

aus $\mathrm{PGL}_2(K)$ bilden also die Klasse des 1-Kozykels $\beta = (b_\rho)$, dessen Bild unter

$$\mathrm{H}^1(G, \mathrm{PGL}_2(K)) \longrightarrow \mathrm{H}^2(G, K^\times)$$

gerade die Kozykelklasse von $f_{\rho,\eta}$ ist.

5.2 Berechnung der definierenden Polynome

Sei $k = \mathbb{Q}$. Für die Erweiterung $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ von k mit Galoisgruppe $G \cong V_4$ ist

$$\vartheta = \sqrt{a} + \sqrt{b} \tag{5.5}$$

ein primitives Element, dessen Minimalpolynom

$$p(X) = X^4 - 2(a+b)X^2 + (a-b)^2 \in \mathbb{Q}[X]$$

ist. Sei

$$F = \mathrm{F}_2([f])$$

der Brauerkörper der Dimension 2 von f. Da

$$K_F = K(T) = \mathbb{Q}(\vartheta)(T) \qquad \text{über} \qquad k_F = F$$

eine zu G isomorphe Galoisgruppe

$$G_F = \{b_\rho \rho \mid \rho \in G\} \tag{5.6}$$

hat und da $K = \mathbb{Q}(\vartheta)$ und F über k linear disjunkt sind, ist ϑ auch primitives Element von $K_F = KF$ über F mit dem Minimalpolynom

$$p_F(T, X) = p(X).$$

Hier taucht die Unbestimmte $T := T_1 \overset{(3.17)}{=} S_1 S_2^{-1}$ also gar nicht auf.

Die Erweiterung $L_F/K(T)$ werde zyklisch vom Grad $p = 2$ gewählt und von dem primitiven Element

$$\gamma_F(T) = \sqrt{c_F(T)}$$

erzeugt. Das Minimalpolynom ist daher

$$q_F(T,X) = X^2 - c_F(T).$$

$c_F(T)$ wird dabei mit Hilfe von Hilbert 90 wie folgt berechnet: Nach Abschnitt 3.4 und nach den Gleichungen (4.6) bis (4.8) ist für ein beliebiges, vom Grad 1 homogenes Element $\lambda(T) \in K(T)$ das Quadrat $\lambda_\rho(T)^2$ von

$$\lambda_\rho(T) \overset{(3.24)}{=} \lambda(T)^{u_\rho - 1} \overset{(3.20)}{=} \lambda(T)^{a_\rho \rho - 1} \qquad (\rho \in G) \tag{5.7}$$

mit

$$f_{\rho,\eta} \overset{(3.27)}{=} \lambda_\rho(T)\, \lambda_\eta(T)^{b_\rho \rho}\, \lambda_{\rho\eta}(T)^{-1} \qquad (\rho, \eta \in G)$$

ein 1-Kozykel von G_F mit Werten in $K(T)^\times$, der nach Satz 2.2 (Hilbert 90) zerfällt.

Zur Vereinfachung der Schreibweise steht im folgenden häufig $\rho \in G_F$ anstelle von $b_\rho \rho \in G_F$. Wird ein solches $\rho \in G_F$ auf ein Element $x \in K$ angewendet, so soll damit die Einschränkung $\rho|_K(x)$ gemeint sein.

Die Konjugierten von

$$\theta := 1 + \sqrt{a} + \sqrt{b} + \sqrt{a}\sqrt{b} \tag{5.8}$$

sind linear unabhängig über $k = \mathbb{Q}$ und bilden somit eine *Normalbasis* von K/k. Wegen der linearen Disjunktheit von K und F sind diese Konjugierten auch eine Normalbasis von $K(T)$ über F. Man setzt (siehe Beweis zu Hilbert 90)

$$\begin{aligned} \beta(T) &:= \sum_{\rho \in G_F} \lambda_\rho(T)^2\, \theta^\rho \\ &= (\lambda_{\mathrm{id}}(T)^2 + \lambda_\sigma(T)^2 + \lambda_\tau(T)^2 + \lambda_{\sigma\tau}(T)^2) \\ &\quad + (\lambda_{\mathrm{id}}(T)^2 - \lambda_\sigma(T)^2 + \lambda_\tau(T)^2 - \lambda_{\sigma\tau}(T)^2)\, \sqrt{a} \\ &\quad + (\lambda_{\mathrm{id}}(T)^2 + \lambda_\sigma(T)^2 - \lambda_\tau(T)^2 - \lambda_{\sigma\tau}(T)^2)\, \sqrt{b} \\ &\quad + (\lambda_{\mathrm{id}}(T)^2 - \lambda_\sigma(T)^2 - \lambda_\tau(T)^2 + \lambda_{\sigma\tau}(T)^2)\, \sqrt{a}\sqrt{b} \end{aligned} \tag{5.9}$$

und

$$c_F(T) := \frac{1}{\beta(T)}, \tag{5.10}$$

so daß

$$\lambda_\rho(T)^2 = \frac{c_F(T)^\rho}{c_F(T)} \qquad (\rho \in G_F) \tag{5.11}$$

gilt.

In Abschnitt 3.4 wurden die Operationen von $\mathrm{GL}_2(K)$ und G auf $K(S_1, S_2)$ erklärt: $\mathrm{GL}_2(K)$ bzw. $\mathrm{PGL}_2(K)$ wirkt auf die Unbestimmten S_1, S_2 bzw. T, während G wie üblich auf den Elementen aus K operiert. Dies ergibt die Operation von G_F auf $K(T)$. Explizit ist

$$\begin{array}{llllllll} S_1^{a_{\mathrm{id}}\mathrm{id}} = S_1, & S_1^{a_{\sigma\sigma}\sigma} = S_1, & S_1^{a_\tau\tau} = S_2, & S_1^{a_{\sigma\tau}\sigma\tau} = S_2, \\ S_2^{a_{\mathrm{id}}\mathrm{id}} = S_2, & S_2^{a_{\sigma\sigma}\sigma} = -S_2, & S_2^{a_\tau\tau} = S_1, & S_2^{a_{\sigma\tau}\sigma\tau} = -S_1 \end{array} \tag{5.12}$$

und wegen $T = S_1 S_2^{-1}$ somit

$$T^{b_{\mathrm{id}}\mathrm{id}} = T, \quad T^{b_{\sigma\sigma}\sigma} = -T, \quad T^{b_\tau\tau} = T^{-1}, \quad T^{b_{\sigma\tau}\sigma\tau} = -T^{-1}. \tag{5.13}$$

Insbesondere erkennt man, daß die Unbestimmte T unter der Operation von G_F nicht invariant bleibt und damit kein Element aus dem Brauerkörper F ist, denn dieser ist gerade der Fixkörper von $K(T)$ unter G_F. Dagegen liegt aber z.B. $T' = T^2 + T^{-2}$ in F (siehe auch Abschnitt 4.5).

Nach (3.22) wähle man ein vom Grad 1 homogenes Element in $K(S_1, S_2)$, etwa

$$\lambda(S_1, S_2) := S_1 + S_2.$$

Aus (5.7), (5.12) und (5.13) folgt damit

$$\begin{array}{lllll} \lambda_{\mathrm{id}}(S_1, S_2) = \dfrac{S_1 + S_2}{S_1 + S_2} & \text{bzw.} & \lambda_{\mathrm{id}}(T) = 1, \\ \lambda_\sigma(S_1, S_2) = \dfrac{S_1 - S_2}{S_1 + S_2} & \text{bzw.} & \lambda_\sigma(T) = \dfrac{T-1}{T+1}, \\ \lambda_\tau(S_1, S_2) = \dfrac{S_2 + S_1}{S_1 + S_2} & \text{bzw.} & \lambda_\tau(T) = 1, \\ \lambda_{\sigma\tau}(S_1, S_2) = \dfrac{S_2 - S_1}{S_1 + S_2} & \text{bzw.} & \lambda_{\sigma\tau}(T) = -\dfrac{T-1}{T+1}. \end{array}$$

Die Quadrate lauten

$$\lambda_{\mathrm{id}}(T)^2 = \lambda_\tau(T)^2 = 1, \qquad \lambda_\sigma(T)^2 = \lambda_{\sigma\tau}(T)^2 = \left(\frac{T-1}{T+1}\right)^2$$

und bilden einen 1-Kozykel von G_F mit Werten in $K(T)^\times$. Man setze

$$\Lambda(T) := \left(\frac{T-1}{T+1}\right)^2. \tag{5.14}$$

Die Operation von G_F auf $\Lambda(T)$ ergibt

$$\Lambda(T)^{\mathrm{id}} = \Lambda(T)^\tau = \Lambda(T) \quad \text{und} \quad \Lambda(T)^\sigma = \Lambda(T)^{\sigma\tau} = \Lambda(T)^{-1} \tag{5.15}$$

Gemäß (5.9) ist

$$\beta(T) = (2 + 2\sqrt{a}) + (2 - 2\sqrt{a})\Lambda(T). \tag{5.16}$$

Nach (5.10) erfüllt der Kehrwert $\beta(T)^{-1}$ die Gleichung (5.11). Ohne Einschränkung kann man allerdings zur Vereinfachung gleich

$$c_F(T) := \beta(T) \tag{5.17}$$

und daher

$$\gamma_F(T) := \sqrt{c_F(T)} \tag{5.18}$$

wählen, da es offensichtlich auf die Erweiterung

$$L_F := K(T)(\gamma_F(T)) = \mathbb{Q}(\vartheta)(T, \sqrt{c(T)}) \tag{5.19}$$

keinen Einfluß nimmt. Dann gilt

$$c_F(T)^{\mathrm{id}} = c_F(T)^\tau = c_F(T) \qquad \text{und} \qquad c_F(T)^\sigma = c_F(T)^{\sigma\tau} = \frac{c_F(T)}{\Lambda(T)}. \tag{5.20}$$

Sei $\mathrm{N}_{K/k} : K \to k : x \mapsto \prod_{\rho\in G} \rho(x) = x\,\sigma(x)\,\tau(x)\,\sigma\tau(x)$ die wie üblich definierte Normabbildung von Zahlkörpererweiterungen. Bei ihrer Fortsetzung auf den Polynomring $K[X]$, die ebenfalls mit $\mathrm{N}_{K/k}$ bezeichnet werde, operiert G trivial auf den Potenzen der Unbestimmten X. Man betrachte nun die Normabbildung

$$\mathrm{N}_{K(T)/F} : \; K(T) \longrightarrow F : \; x \longmapsto \prod_{\rho\in G_F} \rho(x)$$

und ihre ebenso bezeichnete Fortsetzung auf den zugehörigen Polynomring. Die Berechnung des definierenden Polynoms gemäß (4.16) ergibt nämlich nun das definierende Polynom von γ_F über F mit Galoisgruppe $\tilde{G_F}$:

$$\begin{aligned} \tilde{r_F}(T,X) &= \mathrm{N}_{K(T)/F}(q_F(T,X)) \\ &= (X - c_F(T)^{\mathrm{id}})\,(X - c_F(T)^{\sigma})\,(X - c_F(T)^{\tau})\,(X - c_F(T)^{\sigma\tau}) \\ &= (X^2 - c_F(T))^2\;(X^2 - \frac{c_F(T)}{\Lambda(T)})^2 \\ &= [X^4 \;-\; c_F(T)\,(1 + \frac{1}{\Lambda(T)})\;X^2 \;+\; \frac{c_F(T)^2}{\Lambda(T)}]^2 \end{aligned}$$

Auf das Quadrat kann verzichtet werden, da es auf die Bestimmung des Minimalpolynoms ankommt:

$$r_F(T,X) = X^4 \;-\; c_F(T)\,(1 + \frac{1}{\Lambda(T)})\;X^2 \;+\; \frac{c_F(T)^2}{\Lambda(T)} \tag{5.21}$$

Indem man man (5.15) und (5.20) ausnutzt, kann man für die Koeffizienten von $r_F(T,X)$ – sie sind offensichtlich sämtlich aus K_F – nachweisen, daß sie unter der Operation von G_F fix bleiben und damit bereits in F liegen. Dies zeigt $r_F(T,X) \in F[X]$.

Allerdings tritt folgendes Problem auf: Der Koeffizient

$$\begin{aligned} c_F(T)\;(1 + \frac{1}{\Lambda(T)}) &= [(2 + 2\sqrt{a}) + (2 - 2\sqrt{a})\Lambda(T)]\;(1 + \frac{1}{\Lambda(T)}) \\ &= 4 + 2(\frac{1}{\Lambda(T)} + \Lambda(T)) + 2(\frac{1}{\Lambda(T)} - \Lambda(T))\;\sqrt{a} \end{aligned}$$

von X^2 liegt nach Spezialisierung von $T \mapsto t \in \mathbb{Q} - \{\pm 1\}$ genau dann in $\mathbb{Q}$, wenn der $\sqrt{a}$ enthaltende Term verschwindet, d.h. wenn

$$\frac{1}{\Lambda(t)} - \Lambda(t) = 0$$

ist. Für den anderen Koeffizienten $\frac{c_F(T)^2}{\Lambda(T)}$ erhält man dieselbe Bedingung. Sie ist nur für $t = 0$ erfüllt, die andere Lösung $t^2 = -1$ liegt nicht in $\mathbb{Q}$. Dies ist i.a. auch nicht zu erwarten, da die Unbestimmte T nicht aus F kommt, wie bereits bemerkt wurde. Durch geschickten Übergang zu neuen Veränderlichen läßt sich dieses im Einzelfall aber umgehen, indem man zunächst $c := c_F(t)$ berechnet und erst danach

das zugehörige Minimalpolynom ermittelt. Dies wird im nächsten Abschnitt gezeigt. Das Resultat bis hierher lautet:

Satz 5.1

Es sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ eine biquadratische Erweiterung von $k = \mathbb{Q}$ mit zu V_4 isomorpher Galoisgruppe. Dann gibt es für das zentrale Einbettungsproblem, welches durch die Gruppenerweiterung $1 \to \mu_2 \to D_4 \to V_4 \to 1$ gegeben wird, einen virtuellen Lösungskörper

$$L_F = \mathbb{Q}(\vartheta)(T, \sqrt{c_F(T)}),$$

wobei $\vartheta = \sqrt{a} + \sqrt{b}$, $c_F(T) = (2 + 2\sqrt{a}) + (2 - 2\sqrt{a})\,\Lambda(T)$ und $\Lambda(T) = \left(\frac{T-1}{T+1}\right)^2$ sind. Das zugehörige Minimalpolynom über dem Brauerkörper F lautet

$$r_F(T, X) = X^4 \; - \; c_F(T)\,(1 + \frac{1}{\Lambda(T)})\; X^2 \; + \; \frac{c_F(T)^2}{\Lambda(T)}. \qquad \square$$

5.3 Ein Gegenbeispiel zum Hasseschen Normensatz und die Konstruktion von Auflösungskörpern

Sei nun $a = 13$ und $b = -3$, so daß die biquadratische Erweiterung

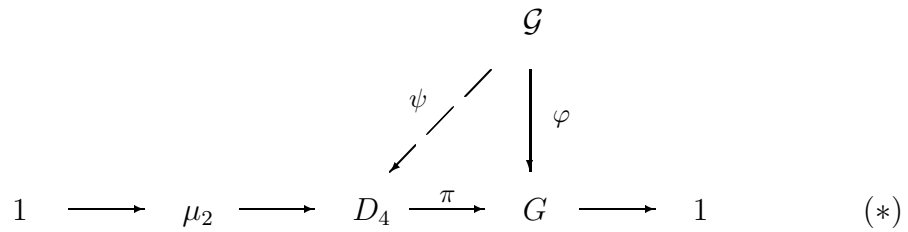
$$\mathbb{Q}(\sqrt{13}, \sqrt{-3})/\mathbb{Q}$$

mit Galoisgruppe $G \cong V_4$ betrachtet wird. Dabei sei G durch $\sigma : \sqrt{13} \mapsto -\sqrt{13}$ und $\tau : \sqrt{-3} \mapsto -\sqrt{-3}$ festgelegt.

Für diese Erweiterung gilt nun nicht das *Hassesche Normenprinzip*: Es gibt nämlich $c \in \mathbb{Q}^\times$, so daß c Norm in allen lokalen Erweiterungen $\mathbb{Q}_p(\sqrt{13}, \sqrt{-3})/\mathbb{Q}_p$, p Primzahl oder $p = \infty$, ist, c aber nicht Norm in der globalen Erweiterung $\mathbb{Q}(\sqrt{13}, \sqrt{-3})/\mathbb{Q}$ ist. Dieses Beispiel wurde von HASSE selbst angegeben (siehe [Has 31], S. 68).

Das Einbettungsproblem (2.15)

(5.22)



ist lösbar, weil die Gleichung (2.17)

$$x^2 - (-3)y^2 = 13$$

für $x = 1, y = 2$ erfüllt ist. Sei

$$Y := T^2 + T^{-2} \tag{5.23}$$

eine Unbestimmte, die – wie im vorherigen Abschnitt (S. 60) bemerkt – in F liegt. X sei eine weitere Unbestimmte, die die algebraische Relation

$$X^2 - bY^2 = a$$

erfülle. Nun spezialisiert man

$$T \longmapsto t := 1, \qquad \text{d.h.} \qquad Y \longmapsto 2 \quad \text{und} \quad X \longmapsto 1.$$

Somit ist nach 5.14 $\Lambda(1) = 0$, wobei man beachte, daß $\Lambda(T)^{-1}$ hier nicht gebraucht wird, so daß die Spezialisierung $t = 1$ überhaupt zulässig ist. Es folgt aufgrund von (5.17)

$$c := c_F(1) = 2 + 2\sqrt{13} \tag{5.24}$$

sowie aufgrund von (5.18)

$$\gamma := \gamma_F(1) = \sqrt{2 + 2\sqrt{13}}. \tag{5.25}$$

$\mathbb{Q}(\sqrt{13}, \sqrt{-3})$ ist tatsächlich ein Teilkörper von $\mathbb{Q}(\pm\sqrt{2 \pm 2\sqrt{13}})$, denn mit $\gamma^\sigma = \sqrt{2 - 2\sqrt{13}}$ ist

$$\begin{aligned}\sqrt{13} &= \frac{1}{2}(\gamma^2-2),\\ \sqrt{-3} &= \frac{1}{4}\gamma\gamma^\sigma.\end{aligned}$$

Der Körper

$$L = K(\gamma) = \mathbb{Q}(\sqrt{13},\sqrt{-3},\sqrt{2+2\sqrt{13}}) = \mathbb{Q}(\pm\sqrt{2\pm 2\sqrt{13}}) \tag{5.26}$$

ist also ein Lösungskörper des gegebenen Einbettungsproblems: Seine Galoisgruppe $\mathrm{G}(L/\mathbb{Q})$ ist isomorph zur Diedergruppe D_4. Das Minimalpolynom von γ über $\mathbb{Q}$ lautet

$$\begin{aligned} r(X) &= \mathrm{N}_{L/\mathbb{Q}}(X-\gamma)\\ &= (X-\sqrt{2+2\sqrt{13}})\,(X-\sqrt{2-2\sqrt{13}})\cdot\\ &\quad\cdot\,(X+\sqrt{2+2\sqrt{13}})\,(X+\sqrt{2-2\sqrt{13}})\\ &= X^4-4\,X^2-48.\end{aligned} \tag{5.27}$$

H. Opolka hat in [Opo 80] das Polynom X^4+X^2-3 angeben, dessen Nullstellen L erzeugen. Diese Koeffizienten unterscheiden sich von denen von $r(X)$ also lediglich um Quadrate aus $\mathbb{Q}$ und das Vorzeichen von X^2. Zusammengefaßt erhält man das folgende Ergebnis:

Satz 5.2

Für die biquadratische Erweiterung $\mathbb{Q}(\sqrt{13},\sqrt{-3})/\mathbb{Q}$ ist

$$L = \mathbb{Q}(\pm\sqrt{2\pm 2\sqrt{13}})$$

ein expliziter Lösungskörper des zu $1\to\mu_2\to D_4\to V_4\to 1$ gehörigen Einbettungsproblems. Das Minimalpolynom über $\mathbb{Q}$ lautet $r(X)=X^4-4X^2-48$. □

Somit ist L aufgrund von [Opo 80], Satz 3 und Abschnitt 4 eine *Auflösung* des *Zahlenknotens*

$$\mathcal{K}(K/k) = \frac{\{c\in k^\times \mid c \text{ ist lokal überall Norm in } K\}}{\{c\in k^\times \mid c \text{ ist globale Norm in } K\}} \le \hat{\mathrm{H}}^0(G,K^\times)$$

von K/k. Mit anderen Worten:

Satz 5.3

Ist $c\in\mathbb{Q}^\times$ Norm in allen lokalen Erweiterungen $\mathbb{Q}_p(\pm\sqrt{2\pm 2\sqrt{13}})/\mathbb{Q}_p$, p Primzahl oder $p=\infty$, so ist c Norm in der globalen Erweiterung $\mathbb{Q}(\sqrt{13},\sqrt{-3})/\mathbb{Q}$. □

5.4 Ein Beispiel zum Satz von Serre

Interessant ist natürlich noch die Frage, wie sich der Satz von SERRE aus der Einleitung in die hier entwickelte Theorie einfügt.

Betrachtet werden dazu die Erweiterungen

$$k = \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{\varepsilon}) \qquad \text{und} \qquad L = \mathbb{Q}(\sqrt{a + b\sqrt{\varepsilon}}) \tag{5.28}$$

mit $G = \mathrm{G}(K/k) \cong \mathbb{Z}/2\mathbb{Z}$. G werde von dem k-Automorphismus $\sigma : \sqrt{\varepsilon} \mapsto -\sqrt{\varepsilon}$ erzeugt. Es gilt nun zu klären, ob das zentrale Einbettungsproblem zur Gruppenerweiterung

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow G \longrightarrow 1 \qquad (**) \tag{5.29}$$

lösbar ist, d.h. unter welchen Bedingungen L/k eine zyklische Körpererweiterung von der Ordnung 4 ist. SERREs Ergebnis spiegelt sich in Satz 1.1 wider.

Nach der Theorie, die in dieser Arbeit entwickelt wurde, ist zunächst einmal der $(**)$ entsprechende 2-Kozykel f berechnen. Dies wurde bereits in [Som 96], S. 74 - 75, Beispiel 1 getan:

(5.30)

$f_{\rho,\eta}$	id	σ
id	1	1
σ	1	-1

Dort wurde auch eine Normgleichung als Kriterium für die Lösbarkeit dieses Einbettungsproblems angegeben (siehe Gleichung (7.4)): Das zu $(**)$ gehörende Einbettungsproblem ist genau dann lösbar, wenn -1 Norm in K ist, d.h. wenn die Gleichung

$$x^2 - \varepsilon y^2 = -1 \qquad \text{(für gewisse } x, y \in \mathbb{Q}\text{)} \tag{5.31}$$

lösbar ist.

Im nächsten Schritt werden die Matrizen gemäß (4.2) ermittelt:

$$(5.32)\qquad \begin{aligned} a_{\mathrm{id}} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & a_{\sigma} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\ a_{\tau} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & a_{\sigma\tau} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

Man wähle wie in Abschnitt 5.2

$$\lambda(S_1, S_2) := S_1 + S_2$$

und

$$\Lambda(T) := \lambda_\sigma(T)^2 = \Big(\frac{T-1}{T+1}\Big)^2.$$

Eine Normalbasis von $\mathbb{Q}(\sqrt{\varepsilon})/\mathbb{Q}$ ist $\{1+\sqrt{\varepsilon},\, 1-\sqrt{\varepsilon}\}$. Es folgt nach (5.9)

$$\beta(T) = (1 + 1\sqrt{\varepsilon}) + (1 - 1\sqrt{\varepsilon})\Lambda(T)$$

sowie nach (5.17) und (5.18)

$$c_F(T) := \beta(T) \qquad \text{und} \qquad \gamma_F(T) := \sqrt{c_F(T)}.$$

Spezialisiert man $T \mapsto t := 1$, so ist

$$(5.33)\qquad \gamma := \gamma_F(1) = \sqrt{1+\sqrt{\varepsilon}},$$

d.h. $a = 1$ und $b = 1$ in der Schreibweise von (5.28).

Wählt man etwa $\varepsilon = \frac{1}{2}$, so ist das Einbettungsproblem (5.29) mit den Parametern $a = 1$, $b = 1$, $\varepsilon = \frac{1}{2}$ lösbar, weil die Bedingung (5.31) mit $x = 1$, $y = 2$ erfüllt ist. Ein Lösungskörper L wird durch

$$(5.34)\qquad L = \mathbb{Q}\Big(\sqrt{1+\sqrt{\frac{1}{2}}}\Big) = \mathbb{Q}\Big(\sqrt{1+\frac{1}{2}\sqrt{2}}\Big)$$

gegeben, der über $K = \mathbb{Q}(\sqrt{2})$ zyklisch vom Grad 2 und über $k = \mathbb{Q}$ zyklisch vom Grad 4 ist.

Das Kriterium

$$a^2 - \varepsilon b^2 = \varepsilon c^2$$

aus Satz 1.1 ist in diesem Fall mit $c = \pm 1$ erfüllt. Bewiesen ist:

Satz 5.4

Für die vom Grad 2 zyklische Erweiterung $\mathbb{Q}(\sqrt{\frac{1}{2}}) = \mathbb{Q}(\sqrt{2})$ von $\mathbb{Q}$ ist

$$L = \mathbb{Q}(\sqrt{1 + \frac{1}{2}\sqrt{2}})$$

ein expliziter Lösungskörper des Einbettungsproblems, welches zu $1 \to \mu_2 \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$ gehört. □

Literaturverzeichnis

[A-T 61] E. Artin, J. Tate: *Class Field Theory.* Cambridge (Mass.): Harvard University 1961

[ArM 82] M. Artin: *Brauer-Severi Varieties.* Brauer Groups in Ring Theory (edited by F. van Oystaeyen, A. Verschoren). Lecture Notes in Mathematics 917. Berlin, Heidelberg, New York: Springer-Verlag 1982

[A-I 95] J. A. De Azcarraga, J. M. Izquierdo: *Lie Groups, Lie Algebras, Cohomology and some Applications in Physics.* Cambridge: Cambridge University Press 1995

[Cha 44] F. Chatelet: *Variations sur un Theme de H. Poincare.* Annales E.N.S. 61 (1944), p. 249 - 300

[Coh 93] H. Cohen: *A Course in Computational Algebraic Number Theory.* Berlin, Heidelberg, New York: Springer-Verlag 1993

[Deu 68] M. Deuring: *Algebren.* Zweite Auflage. Berlin, Heidelberg, New York: Springer-Verlag 1968

[Eck 53] B. Eckmann: *Cohomology of Groups and Transfers.* Annales of Mathematics 58 (1953), p. 481 - 493

[Eke 90] T. Ekedahl: *An Effective Version of Hilbert's Irreducibility Theorem.* Seminaire de Theorie des Nombres, Paris 1988 - 1989 (edited by C. Goldstein). Boston: Birkhäuser (1990), p. 241 - 248

[Had 78] C. R. Hadlock: *Field Theory and its Classical Problems.* The Carus Mathematical Monographs No. 19: The Mathematical Association of America 1978

[Has 31] H. Hasse: *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol.* Nachr. Ges. Wiss. (1931), S. 64 - 69

[Hil 92] D. Hilbert: *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten.* J. reine angew. Mathematik 110 (1892), S. 104 - 129

[Hoe 68] K. Hoechsmann: *Zum Einbettungsproblem.* J. reine angew. Mathematik 229 (1968), S. 81 - 106

[Ike 60] M. Ikeda: *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren.* Hamb. Abh. 24 (1960), S. 126 - 131

[Kan 90] M.-C. Kang: *Construction of Brauer-Severi Varieties and Norm Hypersurfaces.* Can. J. Math., Vol. XLII, No. 2 (1990), p. 230 - 238

[Kar 88] G. Karpilovsky: *Field Theory.* New York, Basel: Marcel Dekker 1988

[Ker 90] I. Kersten: *Brauergruppen von Körpern.* Braunschweig, Wiesbaden: Vieweg 1990

[Lan 83] S. Lang: *Fundamentals of Diophantine Geometry.* New York: Springer-Verlag 1983

[Lan 93] S. Lang: *Algebra.* Third edition. Addison-Wesley Publishing Company 1993

[Lor 92] F. Lorenz: *Einführung in die Algebra, Teil I.* Zweite Auflage. Mannheim, Leipzig, Wien, Zürich: BI-Wissenschaftsverlag 1992 (1987)

[Lor 90] F. Lorenz: *Einführung in die Algebra, Teil II.* Mannheim, Leipzig, Wien, Zürich: BI-Wissenschaftsverlag 1990

[Lor 93] F. Lorenz: *Algebraische Zahlentheorie.* Mannheim, Leipzig, Wien, Zürich: BI-Wissenschaftsverlag 1993

[Mat 88] H. B. Matzat: *Über das Umkehrproblem der Galoisschen Theorie.* Jahresbericht der Deutschen Mathematiker-Vereinigung 90 (1988), S. 155 - 183

[M-Z 55] D. Montgomery, L. Zippin: *Topological Transformation Groups.* New York, London: Interscience 1955

[Neu 69] J. Neukirch: *Klassenkörpertheorie.* Mannheim: Bibliographisches Institut 1969

[Neu 73] J. Neukirch: *Über das Einbettungsproblem der algebraischen Zahlentheorie.* Inventiones math. 21 (1973), S. 59 - 116

[Neu 92] J. Neukirch: *Algebraische Zahlentheorie.* Berlin, Heidelberg: Springer-Verlag 1992

[Opo 80] H. Opolka: *Zur Auflösung zahlentheoretischer Knoten.* Mathematische Zeitschrift 173 (1980), S. 95 - 103

[P-S 92] A. N. Parshin, I. R. Shafarevich (Eds.): *Number Theory II.* Berlin, Heidelberg, New York: Springer-Verlag 1992

[Pie 82] R. S. Pierce: *Associative Algebras.* Berlin, Heidelberg, New York: Springer-Verlag 1982

[Poi 67] G. Poitou: *Cohomologie Galoisienne des Modules Finis.* Paris: Dunod 1967

[Roq 63] P. Roquette: *On the Galois Cohomology of the Projective Linear Group and its Applications to the Construction of Generic Splitting Fields of Algebras.* Math. Annalen 150 (1963), p. 411 - 439

[S-O 80] W. Scharlau, H. Opolka: *Von Fermat bis Minkowski.* Berlin, Heidelberg, New York: Springer-Verlag 1980

[Ser 92] J.-P. Serre: *Topics in Galois Theory.* Research Notes in Mathematics Vol. I. Boston: Jones und Bartlett Publishers 1992

[Ser 94] J.-P. Serre: *Cohomologie Galoisienne.* Lecture Notes in Mathematics 5, Fifth edition. Berlin, Heidelberg, New York: Springer-Verlag 1994 (1973)

[Ser 95] J.-P. Serre: *Local Fields.* GTM 67. Second corrected printing. Berlin, Heidelberg, New York: Springer-Verlag 1995 (1979)

[Sha 94-1] I. R. Shafarevich: *Basic Algebraic Geometry 1: Varieties in Projective Space.* Second edition. Berlin, Heidelberg, New York: Springer-Verlag 1994 (1977)

[Sha 94-2] I. R. Shafarevich: *Basic Algebraic Geometry 2: Schemes and Complex Manifolds.* Second edition. Berlin, Heidelberg, New York: Springer-Verlag 1994 (1977)

[Shz 72] S. S. Shatz: *Profinite Groups, Arithmetic, and Geometry.* Princeton University Press 1972

[Sna 89] V. P. Snaith: *Topological Methods in Galois Representation Theory.* New York: John Wiley & Sons 1989

[Som 96] J. Sommer: *Normgleichungen und Einbettungsprobleme.* Diplomarbeit TU Braunschweig 1996

[Wit 36] E. Witt: *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f.* J. reine angew. Mathematik 174 (1936), S. 237 - 245

Symbolverzeichnis

$\times_G$	Faserprodukt über G, 17
$\otimes_k$	Tensorprodukt über k, 17
$(*)$	Gruppenerweiterung, 13
$[(*)]$	Isomorphieklasse von Gruppenerweiterungen, 15
$\sim$	ähnlich, 17
$A^{\mathcal{G}}$	Fixmodul eines $\mathcal{G}$-Moduls A unter $\mathcal{G}$, 9
$\overline{A}$	zerfallende Erweiterung einer G-Gruppe A mit G, 23
$[A]$	Äquivalenzklasse einer zentral-einfachen k-Algebra A, 17
$A_{\zeta_p}(a,b)$	Normrestalgebra, 20
(a,b)	Quaternionenalgebra, 21
$\mathrm{B}^n(\mathcal{G},A)$	Menge der n-Koränder, 10
$\mathrm{Br}(k)$	Brauergruppe von k, 17
$\mathrm{Br}(k)_p$	Elemente in $\mathrm{Br}(k)$, deren Exponent p teilt, 20
$\mathrm{Br}(K/k)$	relative Brauergruppe von K über k, 18
$\mathbb{C}$	Körper der komplexen Zahlen
$\mathrm{char}\, k$	Charakteristik von k, 2
$\mathrm{C}^n(\mathcal{G},A)$	Gruppe der n-Koketten von $\mathcal{G}$ in A, 9
$C(k)$	Menge der k-rationalen Punkte einer Kurve C, 50
$\dim_k V$	Dimension eines k-Vektorraums V, 28
D_n	Diedergruppe der Ordnung $2n$, 21
Δ^n	Verbindungshomomorphismus, 8
d_n	n-te Korandabbildung, 10

$\mathcal{E}(\mathcal{G}, \varphi, (*))$	Einbettungsproblem, 14
$\mathrm{End}_k(V)$	Ring der k-Endomorphismen eines Vektorraums V, 26
ζ_p	primitive p-te Einheitswurzel, 20
$f_{\sigma_1,\ldots,\sigma_n}$	n-Kozykel, 9
$(f), [f]$	Klasse eines Kozykels f, 10 bzw. 42
F	Teilkörper von $\overline{E}$, 30
$\mathrm{F}_m(\gamma)$	Brauerkörper einer 2-Kozykelklasse γ, 33
$\mathcal{G}$	proendliche Gruppe, 9
$\mathcal{G}_k$	absolute Galoisgruppe von k, 12
$\mathrm{G}(K/k)$	Galoisgruppe von K/k, 9
$\mathrm{G}(g(X))$	Galoisgruppe eines irreduziblen Polynoms $g(X)$, 51
G	endliche Gruppe, 11; oft: Galoisgruppe $\mathrm{G}(K/k)$, 11, 25
G_F	Galoisgruppe $\mathrm{G}(FK/F)$, 34
$\mathrm{GL}_m(K)$	invertierbare $m \times m$-Matrizen mit Koeffizienten in K, 13
$\mathrm{H}^n(\mathcal{K})$	n-te Kohomologiegruppe von $\mathcal{K}$, 7
$\mathrm{H}^n(\mathcal{G}, A)$	n-te Kohomologiegruppe von $\mathcal{G}$ mit Werten in A, 10
$\hat{\mathrm{H}}^n(\mathcal{G}, A)$	n-te Tate'sche Kohomologiegruppe von G in A, 11
$\mathrm{Hom}_k(V, W)$	Menge der k-Homomorphismen von V nach W, 40
$\inf_{\mathcal{G}}^{\mathcal{G}/\mathcal{N}}$	kohomologische Inflation, 11
k	Körper, 1
$\overline{k}$	separabel-algebraischer Abschluß von k, 12
$k_{\mathfrak{p}}$	Komplettierung eines Zahlkörpers k, 20
$k[X]$	Polynomring, 35
$k(T)$	rationaler Funktionenkörper in der Unbestimmten T über k, 32
$k(V)$	Funktionenkörper einer k-Varietät V, 49
K/k	Körpererweiterung, 14
$(K : k)$	Grad von K/k, 29
(K, G, f)	verschränktes Produkt von K und G bezüglich f, 18

$\mathcal{K}$	Komplex, 7
$\mathcal{K}(K/k)$	Knoten von K/k, 65
μ_p	Gruppe der p-ten Einheitswurzeln, 18
$\mathrm{M}_r(k)$	$r \times r$-Matrizen mit Koeffizienten aus k, 17
$\mathbb{N}$	Menge der natürlichen Zahlen
N_G	gruppentheoretische Normabbildung, 11
$\mathrm{N}_{K/k}$	körpertheoretische Normabbildung, 11
$\mathbb{P}_k^m$	projektiver Raum über k, 47
$\mathrm{PGL}_m(K)$	projektive lineare Gruppe von K, 26
$\mathrm{Proj}(R)$	projektive Varietät eines homogenen Koordinatenringes, 48
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{Q}_p$	Komplettierung von $\mathbb{Q}$ bez. der p-adischen Bewertung, 51, 63
$\mathbb{R}$	Körper der reellen Zahlen
$\mathrm{res}_{\mathcal{U}}^{\mathcal{G}}$	kohomologische Restriktion, 11
$\mathrm{res}_{K/k}$	algebrentheoretische Restriktion, 17
$\mathrm{Res}(p, q, Y)$	Resultante der Polynome p und q bezüglich Y, 47
$\rho\|_k$	Einschränkung eines Automorphismus ρ auf k, 59
$\mathrm{s}(A), \mathrm{s}(f)$	Schurindex einer Algebra A bzw. eines Kozykels f, 28
V_4	Kleinsche Vierergruppe ($\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), 21
$\mathrm{V}_m([f])$	Brauer-Severi Varietät, 48
$\mathbb{Z}$	Ring der ganzen Zahlen
$\mathrm{Z}^n(\mathcal{G}, A)$	Menge der n-Kozykeln, 10

Index

Lebenslauf

Name:	Jörn Christian Sommer
Geburtsdatum:	21.10.1969
Geburtsort:	Braunschweig
Eltern:	Institutsleiter Priv. Doz. Dr.-Ing. habil. Claus Sommer und Studienrätin Erika Sommer, geb. Neupauer
Geschwister:	Kirsten Sommer

Schule

1976 - 1980:	Grundschule Lehndorf-Siedlung, Braunschweig
1980 - 1982:	Orientierungsstufe Lehndorf-Ort, Braunschweig
1982 - 1989:	Gymnasium Hoffmann-von-Fallersleben-Schule, Braunschweig
Mai 1989:	Abitur

Zivildienst

1989 - 1990:	Diakonieheim Am Jödebrunnen, Braunschweig

Studium

1990 - 1996:	Mathematik (Diplom) mit Nebenfach Informatik an der Technischen Universität Braunschweig
Juli - September 1991:	Appalachian State University, Boone, North Carolina (USA)
1992:	Vordiplom
1993 - 1994:	University of Cambridge (England)
Juli 1994:	Certificate of Advanced Study in Mathematics with Distinction
Juli 1996:	Diplom

Beruf

Seit Oktober 1996:	Software-Entwickler bei der Siemens AG, Braunschweig

Zusammenfassung

Sei $\mathcal{G}$ eine proendliche Gruppe, und sei $\mathcal{E} = \mathcal{E}(\mathcal{G}, \varphi, (*))$ ein zentrales Einbettungsproblem für $\mathcal{G}$. Ein solches Einbettungsproblem $\mathcal{E}$ ist gegeben durch eine Gruppenerweiterung $(*)\ 1 \to A \to E \xrightarrow{\pi} G \to 1$ endlicher Gruppen mit abelschem Kern A, auf dem G trivial operiert, zusammen mit einem Epimorphismus $\varphi : \mathcal{G} \to G$; gesucht ist ein (surjektiver) Homomorphismus $\psi : \mathcal{G} \to E$ mit $\pi \circ \psi = \varphi$. Ist K/k eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{G}(K/k)$ und ist $\mathcal{G} = \mathrm{G}(\overline{k}/k)$ die absolute Galoisgruppe von k, so ist – galoistheoretisch interpretiert – die Existenz eines solchen surjektiven Homomorphismus ψ gleichbedeutend mit der Existenz einer galoisschen Erweiterung $L/K/k$ mit $\mathrm{G}(L/k) \cong E$.

In dieser Arbeit wird für den Fall, daß $\mathcal{G}$ die absolute Galoisgruppe eines algebraischen Zahlkörpers k ist, ein Verfahren beschrieben, wie man unter gewissen Voraussetzungen im Falle der Lösbarkeit von $\mathcal{E}$ explizit einen Lösungskörper L konstruieren kann. Dabei betrachtet man das Einbettungsproblem zunächst über einem anderen geeigneten Grundkörper, dem sogenannten Brauerkörper F, welcher sich in kanonischer Weise $\mathcal{E}$ zuordnen läßt. Der Körper KF ist ein rationaler Funktionenkörper über K in $m-1$ Unbestimmten $T_1, \ldots, T_{m-1}$, wobei m von $\mathcal{E}$ abhängt, und hat über F eine zu G isomorphe Galoisgruppe. $\mathcal{E}$ erweist sich über F als lösbar. Man konstruiert sodann einen 'virtuellen' Lösungskörper $L_F/KF/F$ für $\mathcal{E}$ mit $\mathrm{G}(L_F/F) \cong E$. Die Lösbarkeit von $\mathcal{E}$ über dem ursprünglichen Grundkörper k selbst werde durch eine rationale Varietät beschrieben: Findet man also mittels diophantischer Methoden einen rationalen Punkt auf dieser Varietät, so ist $\mathcal{E}$ über k lösbar. Gleichzeitig erhält man durch diesen rationalen Punkt eine Spezialisierung für die Unbestimmten $T_1, \ldots, T_{m-1}$, die, wenn man sie in L_F einsetzt, einen expliziten Lösungskörper $L/K/k$ für $\mathcal{E}$ liefert.

Anhand zweier Beispiele (ein Gegenbeispiel zum Hasseschen Normensatz und ein Beispiel zu einem Satz von Serre) wird abschließend gezeigt, wie das Verfahren praktisch funktioniert.

Summary

Let $\mathcal{G}$ be a profinite group, and let $\mathcal{E} = \mathcal{E}(\mathcal{G}, \varphi, (*))$ be a central embedding problem for $\mathcal{G}$. Such an embedding problem $\mathcal{E}$ is given by a group extension $(*)\ 1 \to A \to E \xrightarrow{\pi} G \to 1$ of finite groups with abelian kernel A, on which G operates trivially, together with an epimorphism $\varphi : \mathcal{G} \to G$; then it is searched for a (surjective) homomorphism $\psi : \mathcal{G} \to E$ with $\pi \circ \psi = \varphi$. If K/k is a finite Galois extension with Galois group $G = \mathrm{G}(K/k)$, and if $\mathcal{G} = \mathrm{G}(\overline{k}/k)$ is the absolute Galois group of k, then – in terms of Galois theory – the existence of such a surjective homomorphism ψ is equivalent to the existence of a Galois extension $L/K/k$ with $\mathrm{G}(L/k) \cong E$.

In this work – presuming that $\mathcal{G}$ is the absolute Galois group of an algebraic number field k – a method is described how under certain circumstances and in case of a solvable $\mathcal{E}$ one can explicitly construct a solution L. One first looks at the embedding problem over a different suitable ground field, the so-called Brauer field F, which can be associated to $\mathcal{E}$ in a canonical way. The field KF is a rational function field over K in $m-1$ variables $T_1, \ldots, T_{m-1}$, where m depends on $\mathcal{E}$, and its Galois group over F is isomorphic to G. $\mathcal{E}$ proves to be solvable over F. Then one constructs a 'virtual' solution $L_F/KF/F$ for $\mathcal{E}$ with $\mathrm{G}(L_F/F) \cong E$. Let the solubility of $\mathcal{E}$ over the original ground field k itself be described by a rational variety: So if one finds a rational point on this variety by means of Diophantine methods then $\mathcal{E}$ is solvable over k. With this rational point one simultaneously obtains a specialisation for the variables $T_1, \ldots, T_{m-1}$, which when substituted in L_F gives rise to an explicit solution $L/K/k$ for $\mathcal{E}$.

Finally, two examples (a counter-example to Hasse's norm theorem and an example to a theorem of Serre) show how the method works practically.